

Volunteer and Trustee Privacy Notice

Data controller: Inspire North (Northern) Ltd, 3 Limewood Way, Leeds LS14 1AB

The organisation has appointed Sinead Cregan sinead.cregan@inspirenorth.co.uk as Senior Information Risk Owner (SIRO). The role of the SIRO involves taking ownership of the organisation's information risk policy, acting as an advocate for information risk on the Board and providing written advice to the Accounting Officer on the content of their annual governance statement with regard to information risk.

In addition, we have a Caldicott Guardian (Director of Operations) who is responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing.

1. Background

- 1.1 Inspire North is committed to protecting the privacy and security of your personal information.
- 1.2 This privacy notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the General Data Protection Regulation (GDPR).
- 1.3 It applies to all volunteers and trustees
- 1.4 Inspire North 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 data protection legislation to notify you of the information contained in this privacy notice.
- 1.5 This notice applies to current and former volunteers and trustees. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time.
- 1.6 It is important that you read this notice, together with any other privacy notices 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.

2. Data protection principles

- 2.1 We will comply with data protection law. This says that the personal information we hold about you must be:
 - 2.1.1 used lawfully, fairly and in a transparent way.
 - 2.1.2 collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.

- 2.1.3 relevant to the purposes we have told you about and limited only to those purposes.
- 2.1.4 accurate and kept up to date.
- 2.1.5 kept only as long as necessary for the purposes we have told you about.
- 2.1.6 kept securely.

3. What information does the organisation collect and why?

- 3.1 The organisation collects and processes a range of information about you in a variety of ways. For example, data might be collected through application forms, CVs; obtained from your passport or other identity documents such as your driving licence including from third parties such as references supplied by former employers' and information from criminal records checks permitted by law. We will collect additional personal information in the course of job-related activities throughout the period of you working for us.
- 3.2 Data will be stored in a range of different places, including in your personnel file, in the organisation's HR management systems and in other IT systems (including the organisation's email system).
- 3.3 Inspire North needs to process data to enter into an employment contract with you and to meet its obligations under your employment contract. In some cases, the organisation needs to process data to ensure we are complying with our legal obligations. For example, we are required to check employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled. In other cases, the organisation has a legitimate interest in processing personal data before, during and after the end of the employment relationship.

3.4

Data Item	Reason for Processing	Condition for Processing Volunteer
Your name, address and contact details, including email address and telephone number, date of birth and gender;	Maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency) Ensure effective general HR and business administration;	UK GDPR Article 6(1)(f) – Legitimate interest – required to maintain contact with the volunteer
Recruitment information (references and other information as part of the recruitment process);	Run recruitment and promotion processes. Ensure effective general HR and business administration;	UK GDPR Article 6(1)(b) – processing is necessary for the performance of an agreement with the volunteer
Details of your qualifications, skills, experience and	Provide references on request for current or former employees; and respond to	UK GDPR Article 6(1)(f) – Legitimate interest –

employment history, including start and end dates, with previous employers and with the organisation;	and defend against legal claims. Ensure effective general HR and business administration;	required to maintain contact with the volunteer
Information about your next of kin, dependants and emergency contacts;	To ensure that should anything happen to the individual then the appropriate people can be contacted, and, in some cases, the effective measures can be taken to protect the individual. Ensure effective general HR and business administration;	UK GDPR Article 6(1)(d) – Vital interests
Information about your nationality and entitlement to work in the UK;	To ensure that the individual has the right to work in the UK, which is a legal requirement. Ensure effective general HR and business administration;	N/A - TBC
Copy of driving licence and insurance;	Where the role requires the ability to drive Ensure effective general HR and business administration;	UK GDPR Article 6(1)(f) – Legitimate interest – only where the role requires the ability to drive
Employment records including training records and professional memberships;	To maintain details to evidence that individuals are appropriately trained to undertake the tasks they have been required to do Ensure effective general HR and business administration;	UK GDPR Article 6(1)(f) – Legitimate interest – only in respect that the volunteer is undertaking a role which requires specific training
Information about your use of our information and communication systems;	To ensure that the information and communication systems are being used correctly and not being abused.	UK GDPR Article 6(1)(f) – Legitimate interest – only where the volunteer has been given access
Special Category Data		
Photographs.	To provide effective identification of the individual Ensure effective general HR and business administration;	UK GDPR Article 6(1)(f) – Legitimate interest UK GDPR Article(9)(d) – Legitimate interest
Information about medical or health	Obtain occupational health advice, to ensure that we	UK GDPR Article 6(1)(d) – Vital interests

conditions, including whether you have a disability for which the organisation needs to make reasonable adjustments;	comply with duties in relation to individuals with disabilities, meet our obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled. Ensure effective general HR and business administration;	UK GDPR Article 9(20(C) – Vital interests – to ensure that the volunteer is not placed in a situation that could seriously damage their health or lead to loss of life
Information about your criminal record;	To ensure that any relevant criminal records are dealt with appropriately Ensure effective general HR and business administration;	UK DPA 2018 Schedule 1 part 1 Conditions relating to employment - to undergo a Criminal records check

1. Who has access to data?

- 5.1 Your information may be shared internally, including with members of the HR team (including payroll), your line manager, managers/senior workers in the business and IT staff if access to the data is necessary for performance of their roles.
- 5.2 The organisation shares your data with third parties in order to obtain pre-employment references from other employers, obtain employment background checks from third-party providers and obtain necessary criminal records checks from the Disclosure and Barring Service.
- 5.3 The organisation may also share your data with third parties in the context of a transfer of some or all of its business. In those circumstances the data will be subject to confidentiality arrangements.
- 5.4 We may also need to share your personal information with a regulator or to otherwise comply with the law.
- 5.5 We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so. The organisation also shares your data with third parties that process data on its behalf, in connection with pension, the provision of benefits and the provision of occupational health services.
- 5.6 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.
- 5.7 The organisation will not transfer your data to countries outside the European Economic Area.

2. Which third-party service providers process my personal information?

- 6.1 "Third parties" includes third-party service providers (including contractors and designated agents) and other entities within our group.
- 6.2 The following activities are carried out by third-party service providers, HR Software services, pension administration, IT services, Employee Assistance Programme.

3. How does the organisation protect data?

- 7.1 The organisation takes the security of your data seriously. The organisation has internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties. Please refer to the Information Governance Policy available on INsite.
- 7.2 Where the organisation engages third parties to process personal data on its behalf, we do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

4. For how long does the organisation keep data?

- 8.1 The organisation will hold your personal data for the duration of your office.
- 8.2 The periods for which your data is held after the end of employment are:
 - 8.2.1 Income tax and NI returns, income tax records and correspondence with HMRC Statutory retention period: not less than 3 years after the end of the financial year to which they relate. Statutory authority: The Income Tax (Employments) Regulations 1993 (SI 1993/744) as amended, for example by The Income Tax (Employments) (Amendment No. 6) Regulations 1996 (SI 1996/2631).
 - 8.2.2 National minimum wage records Statutory retention period: 3 years after the end of the pay reference period following the one that the records cover. Statutory authority: National Minimum Wage Act 1998.
 - 8.2.3 Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence - statutory retention period: 3 years after the end of the tax year in which the maternity period ends. Statutory authority: The Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960) as amended.
 - 8.2.4 Wage/salary records (also overtime, bonuses, expenses) Statutory retention period: 6 years. Statutory authority: Taxes Management Act 1970.
 - 8.2.5 Working time records Statutory retention period: 2 years from date on which they were made. Statutory authority: The Working Time Regulations 1998 (SI 1998/1833).

- 8.2.6 Application forms and interview notes (for unsuccessful candidates) - retention period: 1 year. Successful job applicant's documents will be transferred to the personnel file in any event.
- 8.2.7 Assessments under health and safety regulations and records of consultations with safety representatives and committees - retention period: permanently.
- 8.2.8 Inland Revenue/HMRC approvals - retention period: permanently.
- 8.2.9 Money purchase details - retention period: 6 years after transfer or value taken.
- 8.2.10 Parental leave retention period: 18 years from the birth of the child.
- 8.2.11 Pension scheme investment policies - retention period: 12 years from the ending of any benefit payable under the policy.
- 8.2.12 Pensioners' records - retention period: 12 years after benefit ceases.
- 8.2.13 Personnel files and training records (including disciplinary records and working time records) - retention period: 6 years after employment ceases.
- 8.2.14 Redundancy details, calculations of payments, refunds, notification to the Secretary of State - retention period: 6 years from the date of redundancy
- 8.2.15 Senior executives' records (that is, those on a senior management team or their equivalents) - retention period: permanently for historical purposes.
- 8.2.16 Statutory Sick Pay records, calculations, certificates, self-certificates - retention period: 6 years after the employment ceases.
- 8.2.17 Timesheets retention period: 2 years after audit.
- 8.2.18 Trade union agreements - retention period: 10 years after ceasing to be effective.
- 8.2.19 Team Voice Minutes Diversity Minutes - retention period: permanently.

5. How we use particularly sensitive personal information

- 9.1 "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 may process special categories of personal information in the following circumstances:
 - 9.1.1 In limited circumstances, with your explicit written consent.
 - 9.1.2 Where we need to carry out our legal obligations and in line with our Information Security/Governance, Data Protection, Confidentiality and Information Sharing Policy.
 - 9.1.3 Where it is needed in the public interest, such as for diversity/equal opportunities monitoring or in relation to our occupational pension scheme, and in line with Information Security/Governance, Data Protection, Confidentiality and Information Sharing Policy.
 - 9.1.4 Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.
- 9.2 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.

6. Our obligations as an employer

10.1 We will use your particularly sensitive personal information in the following ways:

10.2.1 We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and laws.

10.2.2 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.

10.2.3 We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

7. Information about criminal convictions

11.1 We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our Information Security/Governance, Data Protection, Confidentiality and Information Sharing Policy and Disclosure and Barring Service (DBS) Policy.

11.2 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.

11.3 We are allowed to use your personal information in this way to carry out our obligations Inspire North as meets the requirements under section (2) of the Rehabilitation of Offenders Act (ROA) 1974 to ask exempted questions in relation to specific posts. Applicants who are offered employment with access to children under 18 years of age, vulnerable adults or other positions of trust will be required to complete a criminal records check from the DBS before an appointment can be confirmed. The certificate issued will include details of cautions, reprimands or final warnings, as well as convictions.

8. Automated decision-making

12.1 Employment decisions are not based solely on automated decision-making.

9. Do we need your consent?

- 13.1 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.

10. Change of purpose

- 14.1 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.
- 14.2 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.

11. Your rights

- 15.1 As a data subject, you have a number of rights. You can:
- 15.1.1 access and obtain a copy of your data on request;
 - 15.1.2 require the organisation to change incorrect or incomplete data;
 - 15.1.3 require the organisation to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing;
 - 15.1.4 object to the processing of your data where the organisation is relying on its legitimate interests as the legal ground for processing; and
 - 15.1.5 ask the organisation to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override the organisation's legitimate grounds for processing data.
- 15.2 If you would like to exercise any of these rights, please contact people@inspirenorth.co.uk
- 15.3 You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.
- 15.4 We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

15.5 If you believe that the organisation has not complied with your data protection rights, you can complain to the Information Commissioner.

12. Your duty to inform us of changes

16.1 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.

13. What if you do not provide personal data?

17.1 You have some obligations under your employment contract to provide the organisation with data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith.

17.2 You may also have to provide the organisation with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

17.3 Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable the organisation to enter a contract of employment with you. If you do not provide other information, this will hinder the organisation's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

14. Changes to this privacy notice

18.1 We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.