

Privacy notice for Workers and Associates

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

This privacy notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with data protection legislation.

It applies to you as a member of NFER's temporary workforce. It does not form part of your engagement as a worker.

We may update this notice at any time, and the updated version will be available on the Policy and Training Hub for Workers and Associates.

1 Who is responsible for deciding how your information is processed?

NFER is the data controller, responsible for deciding what personal data is collected and how it is used, before, during and after your deployment. If you have any queries, please contact HR.

We may use data processors to provide specific services; details are provided in section 9.

2 What personal data do we hold about you?

We will collect, store, and use the following categories of personal information about you:

- personal contact details such as name, title, addresses, telephone numbers, and personal email addresses
- date of birth
- National Insurance number
- bank account details, payroll records and tax status information
- rates of pay, and pension information
- the dates and details of your engagement or deployment (including roles and any training carried out)
- recruitment information (including copies of right-to-work documentation, references and other information included in a CV or cover letter or as part of the application process)
- evidence of a satisfactory DBS check (the certificate number and date of issue) or equivalent where appropriate for your role
- compensation history
- performance/complaint related information
- CCTV footage and other information obtained through electronic means such as swipe card records
- information about your use of our library, information and communications systems

- images, (both photographs and videos) audio and visual recordings of meetings, training or briefings made in the course of your work (you will be informed prior to the start of any recording)
- other relevant knowledge, skills and experience
- conflicts of interest outside NFER where relevant.

We may also collect, store and use the following more sensitive types of personal information:

- Information about your ethnicity, religious beliefs, gender identity, sexual orientation, disability, neurodiversity and socioeconomic status
- Information about your health, including any medical condition and / or disability, health and sickness records, including
 - dietary requirements
 - details of any absences (other than holidays)
- Biometric information (used as part of Microsoft's authentication tool and is only stored on your phone and never sent to Microsoft or NFER).
- Information about criminal convictions and offences.

In the event of an exceptional circumstance, you may be asked to provide additional personal or special data. Such data would only be used whilst the event is underway and to address a specific business need. Most of the personal data you provide is held in NFER's Human Resources Enterprise Software. HR also maintain folders of worker information.

3 How do we collect your personal data?

We collect personal information about you through the expression of interest, application and recruitment process, either directly or from a recruitment agency. We may sometimes collect additional information from third parties including former employers or other background checks.

We will collect additional personal information in the course your deployments by NFER.

4 What do we do with the general category personal data held about you?

We will only use your personal information when the law allows us to. NFER endeavours to ensure that your personal data is stored in the UK (or EEA). Where it is stored outside of these regions, we ensure appropriate safeguards are in place.

Human resources

HR will use your personal data for the following:

- making a decision about your appointment or deployment to an Assignment using your CV, application form/expression of interest and records of qualifications
- determining the terms on which you work for us
- checking you are legally entitled to work in the UK
- sharing regular updates in the Associates Newsletter

- paying you and, if you are paid via PAYE, deducting tax and National Insurance contributions (NICs)
- auto-enrolling you in a pension arrangement in accordance with our statutory automatic enrolment duties
- administering the worker contract we have entered into with you
- business management and planning, including accounting and auditing
- managing performance and determining performance requirements including decisions about rates of pay
- gathering evidence for possible performance-related reviews
- making decisions about your continued deployment and/or engagement
- making arrangements for the termination of your worker relationship
- training and development requirements
- dealing with legal disputes involving you, or other employees, workers or contractors, including accidents at work.

IT facilities

If required, your name is used to set up your IT and telephone accounts, and your name and other organisational information (role, department etc.) is stored in Active Directory. Details of your deployment are used to set permissions for data access. Although biometric data will be required for multifactor authentication, it will not be shared with NFER or Microsoft.

If you raise an IT helpdesk ticket, your name is recorded and is used to contact you about the ticket.

There may be circumstances when the Foundation requires access to your e-mail account or details of your internet use from NFER equipment. Under the Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-Keeping Purposes) Regulations 2018, NFER's Senior Management Team reserves the right to monitor e-mails, voicemails, internet access and telephone calls. Full details are provided in section 7 of the Data Security Policy for Associates.

Core business activities

Your personal information may be used to support the Foundation's core business activities, for example, with your permission your CV may be used in proposals, or your image included in promotional material on the NFER website or other relevant sites (for example LinkedIn). Note: where personal information is included in a published contract, the Foundation will, wherever possible redact this prior to publication. Where necessary your personal data may be used to access cloud-based software, training and development activities or other services required to support you in delivering your role. It may be necessary to share your details with the company who provides NFER with travel, professional indemnity and public liability insurance.

You may also choose to share information about yourself with colleagues as part of NFER's internal communication strategy. This may be available on the intranet or via NFER's online social network (Microsoft's Viva Engage).

Your address may be shared with project teams for the purpose of distributing materials required during an Assignment.

Site security

In the Slough Office, the Foundation operates in a secure working environment. The grounds are completely fenced and are monitored by closed-circuit television. Your image is recorded by the CCTV footage. Contact Facilities for further details.

All entrances to the building are secured and can only be used by authorised staff using a swipe card system. The swipe cards are linked to individuals and data about when they are used is recorded. This data may be used to monitor worker presence in the office.

Wellbeing and support services

Workers have the option to share with HR details of any medical conditions (for example allergies, diabetes), long-term health conditions or a registered disability. Sharing this information may help to assist if the person concerned is taken ill unexpectedly, needs assistance during an evacuation of the building, or experiences any adverse re-action or complications as a consequence of their condition. It is held securely and confidentially in NFER's HR Enterprise Software. This type of information may be shared with the First Aid Coordinator who is responsible for drafting any plan to deal with situations that may arise from the condition.

NFER's Safety Health and Environment Policy aims to ensure the health and safety of its workforce, visitors and contractors and to minimise the environmental impact of our activities. It has a number of policies which could lead to the collection of personal data.

5 What is the legal basis for processing general category personal data?

The table below sets out the situations in which we will process your personal information and the legal basis we rely for that processing.

Consent	Use of your image (photo or video)
UK GDPR article 6 (1) (a)	
to perform our contract with you	Making a decision about your appointment and deployment to an Assignment using your CV, application form and records of qualifications
UK GDPR article 6 (1) (b)	
	Determining the terms on which you work for us
	Administering the worker contract we have entered into with you
	Making decisions about rates of pay
	Making decisions about your continued engagement or deployment to an Assignment

	Making arrangements for the termination of our working relationship
to enable us to comply with legal obligations	Checking you are legally entitled to work in the UK and validating your right to work
UK GDPR article 6 (1) (c)	Paying you and, if you are paid via PAYE, deducting tax and National Insurance contributions (NICs)
	Enrolling you in a pension arrangement in accordance with our statutory automatic enrolment duties
	Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work
	Complying with health and safety obligations
	To prevent fraud
	Equal opportunities monitoring
to pursue legitimate interests	Core business activities including management and planning, accounting and auditing
UK GDPR article 6 (1) (f)	Providing facilities such access to IT and library services
	Managing performance and determining performance requirements
	Gathering evidence for possible performance-related reviews
	Education, training and development requirements
	Monitoring sickness absence
	To monitor your use of our library, information and communication systems to ensure compliance with our IT policies

To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution

To conduct data analytics studies to review and better understand worker deployment, retention and attrition rates

Maintaining site security

Where NFER relies on legitimate interest as its legal basis, we have carried out a legitimate interest assessment, which demonstrates that the evaluation fulfils one of NFER's core business purposes (administering NFER's day-to-day business). It cannot be done without processing your personal data, but processing does not override your interests.

Change of purpose

We will only use your personal information for the purposes for which we collected it unless 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.

6 How does NFER use special category personal data?

Special category personal data (information about your health, racial or ethnic origin, sexual orientation) requires higher levels of protection. We need to have further justification for collecting, storing and using it. NFER has an appropriate policy document (contact the Compliance Officer) which sets out how it is protected when processed to meet legal obligations.

Situations in which we will use your sensitive personal information

In general, we will not process particularly sensitive personal information about you unless it is necessary for performing or exercising obligations or rights in connection with your worker status.

On rare occasions, there may be other reasons for processing, such as it is in the public interest to do so. The situations in which we will process your particularly sensitive personal information are listed below.

- We will use evidence of a satisfactory DBS check or equivalent at the appropriate level for your role as it is a requirement of the role.
- We will use information about your physical or mental health, disability status and racial or ethnic origin (insofar as it relates to particular health risks) to ensure your health and safety in the workplace, to provide appropriate workplace adjustments, and to monitor sickness absence. We need to process this information to exercise rights and perform obligations in connection with your worker status.

- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your gender or sexual life or sexual orientation or health to ensure meaningful monitoring and reporting of Equality, Diversity and Inclusion (EDI) data and development of policies in this area.
- You share special category personal data on NFER's internal communication platforms.

Information about criminal matters and being struck off the teaching register

In the event of unsatisfactory DBS checks we may hold information about unspent criminal convictions, charges, pending prosecutions, cautions. If relevant, we may also maintain a record that you are a barred teacher.

We will only collect information about such matters if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect this information 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, or have received information from reliable sources such as STA. We will use this information to determine if it is lawful or appropriate for you to continue in your role.

7 What is the legal basis for processing special category personal data?

The table below sets out the situations in which we will process your special category personal data and the legal basis we rely on for processing.

Employment law UK GDPR article 9 (2) (b)	Equal opportunity and diversity monitoring
Occupational health UK GDPR article 9 (2) (h)	managing HR procedures for administering sick pay and sick leave schemes, managing absence, administering maternity, paternity, adoption and shared parental leave and related pay schemes
	Monitoring absence managing a safe and secure working environment
Made public by the data subject UK GDPR article 9 (2) (e)	Anything you chose to share on NFER's internal platforms

8 Automated decision-making

We do not envisage that any decisions will be taken about you using automated means, however we will notify you if this position changes.

9 Who will your personal data be shared with?

We will only share your personal information with third parties where required by law or to administer our working relationship with you. This means we may share your personal data with amongst others, our payroll provider (IRIS), pension provision, cloud-based IT services, and training providers. Your personal information may be used to support the Foundation's core business activities, for example your CV may be used in proposals and therefore your details could be shared with clients, partners, Associates or research participants to deliver our work.

The list below provides details of the categories of data processors used by NFER to process staff personal data

- payroll providers, such as IRIS
- Human Resources Enterprise Software
- pension providers, such as the People's Pension
- external survey providers
- IT systems and software
- training providers
- clients and partners
- providers of identity and criminal records checks
- regulatory bodies within the country you are based, including HMRC, the Charity Commission
- and Companies House (dependent on role).
- outsourced payroll and other service providers for those based outside the UK.

For details of these processors, please contact the Compliance Officer (compliance@nfer.ac.uk).

When we use third party data processors to process your data, we have contracts in place with them. This means that they should not do anything with your personal information unless we have instructed them to do it. They will not share your personal information unless it is authorised by NFER. The security arrangements of these third parties have been reviewed and deemed acceptable. They will hold it securely and retain it for the period we instruct.

NFER uses processors who store personal data in the UK or European Economic Area (EEA) wherever possible. If transfer outside these areas is necessary, its transfer will be protected by the use of an appropriate safeguard.

In certain situations, other interested parties (for example the schools we ask you to visit) may request evidence of a clean DBS certificate. The interested party may be provided with your 12 digit certificate number and date of issue in advance of your visit.

There are specific requirements for accessing NPD data via the Office for National Statistics Secure Research Service (ONS SRS). It may be necessary to share personal data to meet their requirements.

10 How is the security of your data maintained?

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. NFER demonstrates its commitment to maintaining the confidentiality, integrity and availability of personal data with certification to ISO 27001, the international standard for information security.

In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions, and they are subject to a duty of confidentiality. Details of these measures may be obtained from the Compliance Officer (compliance@nfer.ac.uk).

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.

11 How long will my personal data be kept?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. 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 requirements. Full details are provided in the Deletion and Retention Policy (available on request).

If in the event of exceptional circumstances, you have been asked to provide additional personal information, it will be deleted once it is no longer needed.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.

12 What rights do I have over my personal data?

It is important that the personal information we hold about you is accurate and current. Temporary workers and Associates are encouraged, at least annually, to contact associates@nfer.ac.uk to update any person information in our records.

Your rights in connection with personal information NFER handles your personal data in accordance with the rights given to individuals under data protection legislation. The rights available to you depend on our reason for processing your information. You have the right to:

- Request access to your personal information (commonly known as a "subject access request"). This enables you to receive a copy of the personal information we hold about you. There are some exemptions, which means you may not always receive all the information we process.
- Request correction of the personal information 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 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. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- Object to processing of your personal information 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. You also have the right to object where we are processing your personal information for direct marketing purposes.
- Request the restriction of 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.
- Request the transfer of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the Compliance Officer (compliance@nfer.ac.uk).

What we may need from you

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.

Right to withdraw consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Compliance Officer (compliance@nfer.ac.uk). 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.

13 Who can I contact about how my data is processed?

NFER's Head of Data Security, supported by a Compliance Officer, oversees compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the Compliance Officer in the first place or you can follow the process outlined in the [Complaints Policy](#). After we have responded, 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.

14 Updates

We keep our privacy notice under regular review to make sure it is up to date and accurate; any changes will be recorded.

This privacy notice was updated in November 2023 to reflect changes to some of NFER's third party data processors, the use of Microsoft 365 and the introduction of NFER's internal social network.

This privacy notice was updated May 2024 to clarify how NFER processes information about staff background characteristics such as social background, sexual orientation, religious beliefs, ethnicity, and disability.

This privacy notice was reviewed and updated in September 2025, to update information related to NFER's payroll provider and HR Enterprise Software.

This privacy notice was updated in July 2026 to cover data protection complaints.