

Employee Privacy Notice

Doc No: IMSP01

Version:12

Date: March
2023

Introduction

The Nuclear Decommissioning Authority (NDA) 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 the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA).

We are registered as a Data Controller with the Information Commissioner's Office (ICO). Our registration number is Z9273030. 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.

This notice applies to current and former employees, workers and contractors. It does not form part of any contract of employment or other contract to provide services. We may update this notice at any time.

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

For further details please refer to the NDAs [Personal Information Charter](#)

Our Contact Details

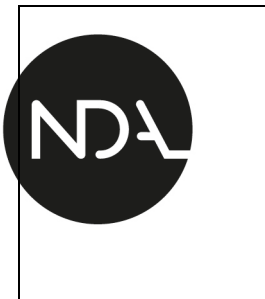
Data Protection Officer (DPO)
Nuclear Decommissioning Authority (NDA)
Herodus House
Westlakes Science & Technology Park
Moor Row
Cumbria
CA24 3HU
Email: dpo@nda.gov.uk

The type of personal information we collect

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 identity has been removed (anonymised data). There are certain types of more sensitive personal data (special category data) which require a higher level of protection, such as information about a person's health or criminal convictions.

We may 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;


	Employee Privacy Notice	
	Doc No: IMSP01	Version:12 Date: March 2023

- Date of birth;
- Gender;
- Marital status and dependants;
- Next of kin and emergency contact information;
- National Insurance number;
- Bank account details, payroll records and tax status information;
- Job title;
- Salary, annual leave, pension and benefits information;
- Start date and, if different, the date of your continuous employment;
- Leaving date and your reason for leaving;
- Location of employment or workplace;
- Copy of driving licence and car insurance;
- 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);
- Employment records (including job titles, work history, working hours, holidays, training records and professional memberships);
- Compensation history;
- Performance information;
- Disciplinary and grievance information;
- Information about your use of our information and communications systems;
- CCTV images used to monitor access to buildings etc;
- Photographs;
- Passport details (including number, expiry date and place of issue);
- Computer username from NDA Network (used as a unique identifier);
- Username, work number and title (for on-premise deployment of Windows 10 and Office 365);
- Personal data related to the online training platform (including full name; corporate email address; module undertaken; completion status; assessment status; date undertaken & performance analytics);
- Electronic signatures
- Responses to staff surveys (only if this data is not anonymised)

Please note, the above list is not exhaustive.

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

- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions for equality and diversity monitoring purposes;
- Trade union membership;
- Information about your health, including any medical condition, health and sickness records, reasonable/workplace adjustment records etc.;

	Employee Privacy Notice		Version:12
	Doc No: IMSP01		Date: March 2023

- details of any absences (other than holidays) from work including time on statutory parental leave and sick leave; and
- Information about criminal convictions and offences.
- Biometric data, including fingerprint authorisation to access IT systems

How we get the personal information and why we have it

We collect personal information about employees, agency workers and contactors through the application and recruitment process, either directly from candidates or sometimes from an employment agency. We may sometimes collect additional information from third parties including former employers, credit reference agencies or background check agencies.

We will collect additional personal information in the course of job-related activities throughout the period that you work for us and will only use your personal information when the law allows us to. The lawful basis for processing your personal data depends on the processing activity and we rely on the following lawful basis for processing your personal data under the UK Data Protection Act 2018/UK GDPR:


- Article 6(1)(a) where we have your consent;
- Article 6(1)(b) which relates to processing necessary for the performance of a contract;
- Article 6(1)(c) so we can comply with our legal obligations as your employer;
- Article 6(1)(d) in order to protect your vital interests or those of another person;
- Article 6(1)(e) for the performance of our public task;
- Article 6(1)(f) for the purposes of our legitimate interest. (In accordance with best practice a Legitimate Interests Assessment (LIA) will always be conducted when this lawful basis is used)

Special category data

Where the information we process is special category data, for example our health data, the additional bases for processing that we rely on are:

- Article 9(2)(b) which relates to carrying out our obligations and exercising our rights in employment and the safeguarding of your fundamental rights.
- Article 9(2)(c) to protect your vital interests or those of another person where you are incapable of giving your consent.
- Article 9(2)(h) for the purposes of preventative or occupational medicine and assessing your working capacity as an employee.
- Article 9(2)(f) for the establishment, exercise or defence of legal claims.
- Article 9(2)(j) for archiving purposes in the public interest.

In addition, we rely on processing conditions in Schedule 1 part 1 paragraph 1 and Schedule 1 part 1 paragraph 2(2)(a) and (b) of the DPA2018. These relate to the

		
	Employee Privacy Notice Doc No: IMSP01	Version:12 Date: March 2023

processing of special category data for employment purposes, preventative or occupational medicine and the assessment of your working capacity as an employee.

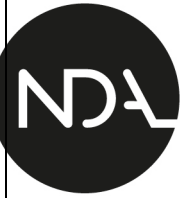
Please see the 'Your data protection rights' section for more information on withdrawing your consent.

What we do with the information

Information related to your employment, conduct, performance & training:

- Making a decision about your recruitment or appointment;
- Determining the terms on which you work for us;
- Security vetting, including aftercare
- Checking you are legally entitled to work in the UK;
- Paying you and, if you are an employee or deemed employee for tax purposes, deducting tax and National Insurance contributions (NICs);
- Providing the following benefits to you:
 - Annual leave entitlement
 - Pension scheme
 - Maternity and Paternity leave and pay
 - Cycle to work scheme
 - Car lease scheme
- Administering the contract we have entered into with you;
- Assessing your performance at work, e.g. probation reviews, PDR's, pay & grading reviews etc;
- Education, training and development needs required for your role;
- Making decisions about your continued employment or engagement;
- Making arrangements for the termination of our working relationship;
- Ascertaining your fitness to work, managing sickness absence, keeping in touch during an absence and enabling workplace adjustments;
- Dealing with any employer/employee related disputes;
- Gathering evidence for grievances and respect at work matters and investigations to which you may be a party or witness;
- Whistleblowing concerns raised by you, or to which you may be a party or witness;
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work;
- Disciplinary processes/procedures and documentation related to any investigations, hearings and warnings/penalties issued;
- Complying with Legal Obligations, including but not limited to, health and safety obligations;
- Meeting the training and development needs required for your role.

Other situations in which we will process your personal information are listed below (please note, this list is not exhaustive):



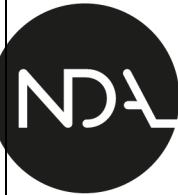
Employee Privacy Notice

Doc No: IMSP01

Version:12

Date: March
2023

- Business management and planning, including accounting and auditing;
- For official purposes; or in the exercise of a function as a Public Authority and Arm's Length Body of BEIS as a government department;
- To prevent fraud;
- To make travel arrangements, via a third party data processor, with organisations who provide travel services;
- To monitor your use of our 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 employee retention and attrition rates;
- Equal opportunities monitoring;
- To create records in, and allow access to, the cloud based learning management system (LMS);
- To allow desktop transformation from Windows 7 to Windows 10 and Office 365;
- To protect staff from the health risks of working with display screen equipment (DSE), such as PCs, laptops, tablets and smartphones;
- To identify potential locations for hub offices. Following the Covid-19 shut down we would like to identify possible sites for hub offices which would support our employees working in a more flexible way. To determine which locations might be appropriate for consideration, it is necessary for us to understand the 'heat map' of areas where our employees currently live, compared to our existing offices;
- To comply with instructions and directions from Government, including requirements to increase openness and transparency in organisations performing public tasks and provide public assurance regarding use of taxpayers' money. For example:
 - we share with the Cabinet Office the names, job titles and details of salaries and allowances of employees who earn £150,000 or more per annum. The Cabinet Office then externally publish that information in bands of £5,000 along with details of other senior civil servants in accordance with freedom of information principles. More detail is provided in the document 'Cabinet Office High Earners List – Employee information sheet'. You have the right to object to this processing as explained in the 'Your data protection rights' section below;
 - for those earning in excess of £127,750 pro rata between 30 September 2021 and 31 January 2022, and/or any performance related pay above £17,500 (also pro rata for the same period), we have been asked to provide the HM Treasury (HMT) with certain details. The request does not ask for your personal name, address or date of birth but it does ask for contracted hours, contract type, pay, performance related pay, employer pension contributions, allowances, job titles and employer. This information is required in order to assess the effectiveness of the Guidance for Approval of Senior Pay and to create a public sector

	Employee Privacy Notice		Version:12
	Doc No: IMSP01		Date: March 2023

benchmarking tool. HMT have drafted a separate Privacy Notice to cover this processing, which contains details on how to contact their DPO.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your 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).

Disclosures under the Freedom of Information Act (FoIA) - As a public authority we receive information requests under the FoIA (2000) about our staff and we must consider whether to disclose staff information (including agency and temporary staff) in response to these requests. Please refer to [CSPR01 - Information request handling procedure](#) for more detail on how we handle FOI requests.

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.

Do we need your consent?

We do not need your consent if we use special category personal data 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, including criminal conviction information held outside of the UK, if it is appropriate given the nature of the role and where we are legally able to do so. The information will be collected as part of the recruitment process or we may be notified directly by yourself or a third party in the course of you working for us.

		
	Employee Privacy Notice Doc No: IMSP01	Version:12 Date: March 2023

All processing will be in line with our data protection policy and adhere to prevailing data protection legislation.

Automated decision-making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. The NDA does not currently make any automated decisions about its staff.

How we store your information

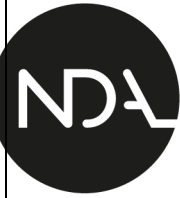
We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

Who will have access to your personal data

We limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. For example: Government departments including BEIS; Government Agencies, including Government Communications Headquarters (GCHQ) & the National Cyber Security Centre (NCSC); other NDA group businesses including Sellafield, Magnox, Dounreay, Nuclear Waste Services (Low Level Waste Repository and Radioactive Waste Management) & Nuclear Transport Solutions (International Nuclear Services & Direct Rail Services); and data processors who operate on the NDAs behalf. We require all data processors to enter into agreements that satisfy the requirements of Article 28 of the GDPR. Further details on these measures may be obtained from the Data Protection Officer.

The following activities are carried out by third-party service providers:

- Regulators (e.g. HMRC)
- Pension administration (Following transfer to the new iTrent Payroll Managed Service some legacy data will still be stored by CGI for administration and contractual obligations. It will be retained until such time as it is no longer required and will then be securely destroyed);
- Benefits provision (Edenred);
- Online platform to deliver and manage training modules to ensure staff can perform their job within the expected organisational requirements. This online platform is managed by a third party provider called "QA" who have partnered with a company called "Cornerstone" that hosts Learning Management System (LMS), this is a cloud based service using the SaaS service model;
- Occupational health (UK Screening Solutions);
- Trade union membership;
- Travel arrangements (Click Travel for air, rail, hotels etc & Enterprise Rent-A-Car



Employee Privacy Notice

Doc No: IMSP01

Version:12

Date: March
2023

- for hire vehicles);
- On-line DSE assessments for agile workers;
- Some network & information security activities.

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.

We may also transfer your personal data outside of the EU/EEA. If this is the case you can expect a similar degree of protection in respect of your personal information.

We will only hold onto your personal information for as long as necessary to fulfil the purposes we collected it for. All records are retained and securely destroyed in accordance with [IMG02 - NDA Records Retention Schedule](#). However, your information may be held beyond the specified retention periods where there is the potential for it to fall under the remit of ongoing government independent inquiries.

Testing IT Systems

In exceptional circumstances the NDA may use live data to test IT systems. Permission to use live data is by exception only & a valid business case must be approved by the NDA Chief Information Security Officer (CISO), Data Protection Officer (DPO), relevant Information Asset Owner (IAO) and Senior Information Risk Owner (SIRO).

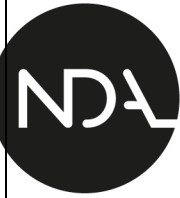
All test data will be protected to the same standard as live data. Appropriate security precautions and permissions will be applied, data won't be used for any purpose other than for testing and all copies will be deleted as soon as the testing is complete.

Your data protection rights

New data protection legislation strengthens the rights of individuals and includes:

- The right to be informed (which this notice fulfils);
- The right of access;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object;
- Rights in relation to automated decision making and profiling.

For a detailed explanation of these rights, and the specific circumstances in which they apply, please visit the Information Commissioners Office (ICO) [website](#)

**Employee Privacy Notice****Doc No: IMSP01**

Version:12

Date: March
2023

If you wish to exercise any of your rights, including where you are seeking a copy of your own personal information, please contact the DPO via dpo@nda.gov.uk

How to complain

If you wish to make a complaint to the NDA about the way in which we have processed your personal information please contact the DPO using the email address above.

If you remain dissatisfied with the response received, you have the right to lodge a complaint to the ICO. The ICO is the UK's independent body set up to uphold information rights, and they can investigate and adjudicate on any data protection related concerns you raise with them. They can be contacted at:

Information Commissioner's Office
Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
0303 123 1113
ico.org.uk

Record Description: Privacy Notice

Record Owner: Jo Doran – Information Governance

Record Format: Electronic/Hardcopy