NOC All Staff Privacy Notice

The National Oceanography Centre (NOC) is committed to protecting the privacy and security of your personal information and being transparent about what we do with it.

This privacy notice describes how NOC collect and process data about you during and after your employment. This Privacy Notice applies to current and former employees only.

Overview

This Privacy Notice describes the categories of Personal Data that we collect, how we use your Personal Data, how we secure your Personal Data, when we may disclose your Personal Data to third parties, and when we may transfer your Personal Data outside of your home jurisdiction. This Privacy Notice also describes your rights regarding the Personal Data that we hold about you including how you can access, correct, and request erasure of your personal data.

We will only process your Personal Data in accordance with this Privacy Notice unless otherwise required by applicable law. We take steps to ensure that the Personal Data that we collect about you is adequate, relevant, not excessive, and processed for limited purposes.

NOC is required by law to provide you with the information in this notice. This notice has been designed to meet the requirements of the UK Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation ("UK GDPR") (collectively referred to in this Privacy Notice as Data Protection Law).

What personal information does NOC process?

For the purposes of this Privacy Notice, Personal Data means any information about an identifiable individual ("Personal Data"). Personal Data excludes anonymous or de-identified data that is not associated with a particular individual. To carry out our activities and obligations as an employer, we may collect, store, and process the following categories of Personal Data, which we require to administer the employment relationship with you:

- information provided by you such as your name, address and contact details, including email address and telephone number, date of birth and gender.
- the terms and conditions of your employment.
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with NOC.
- information about your pay and benefits.

- details of your bank account and national insurance number.
- marital and dependent status, when needed to administer benefits such as health insurance or pension benefits.
- wage and benefit information.
- information about your next of kin and emergency contacts.
- information about your nationality and entitlement to work in the UK.
- professional memberships
- information from references.
- Photograph
- information on Disclosure and Barring Service (DBS) checks including the outcome of the checks (see section below on Collection and Use of Special Categories of Personal Data and Criminal Conviction Data).
- details of your work pattern (days of work and working hours).
- details of periods of leave taken by you, including holiday, sickness and other absence, and the reasons for the leave.
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence.
- performance management information, including annual appraisals, performance development reviews (PDR) and ratings, training you have participated in, performance improvement plans and related correspondence.
- information about medical or health conditions, including whether or not you have a disability for which the organisation needs to make reasonable adjustments (see section below on Collection and Use of Special Categories of Personal Data and Criminal Conviction Data).
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief (see section below on Collection and Use of Special Categories of Personal Data and Criminal Conviction Data).
- other personal details included in a CV, resume, application form or cover letter or that you otherwise voluntarily provide to us.
- other relevant information as applicable required by NOC in order to ensure we fulfil our obligations as an employer.
    - images captured on CCTV, Body Worn Video (Southampton site only) and Automatic numberplate recognition (Southampton site only). Further information on NOC's use of CCTV can be found in the Surveillance Camera Procedure Policy.

The Personal Data listed in this Privacy Notice is required in order for us to administer the

employment relationship. Failure to provide or allow us to process mandatory Personal Data may affect our ability to accomplish the purposes stated in this Privacy Notice.

NOC collects this information in a variety of ways.
For example, data is collected through application forms and CVs; obtained from your passport or other identity documents; from forms completed by you at the start of or during employment (such as benefit nomination forms); from correspondence with you; or through interviews, meetings or other assessments.

We will collect the majority of the Personal Data that we process directly from you. In limited circumstances third parties may provide your Personal Data to us, such as former employers, official bodies (such as regulators or criminal record bureaus) and medical professionals.

You are able to directly update some of the information held on your record on NOC's Business Information System and to view the other fields in your record.

Data is stored in a range of different places, including in your electronic personnel file, in NOC's Business Information System, and across other IT systems (including the organisation's network drives and email system).

Use of Personal Data
We only process your Personal Data where Data Protection Law permits or requires it, including where the processing is necessary for the performance of our employment contract with you, where the processing is necessary to comply with a legal obligation that applies to us as your employer, for our legitimate interests or the legitimate interests of third parties, to protect your vital interests, or with your consent if applicable law requires consent. We may process your Personal Data for the following legitimate business purposes and for the purposes of performing the employment contract with you:

- Employee administration (including payroll and benefits administration).
- Business management and planning.
- Processing employee work-related claims (for example, insurance and worker's compensation claims).
- Accounting and auditing.
- Conducting performance reviews and determining performance requirements.
- Assessing qualifications for a particular job or task.
- Internal or external investigations.
- Gathering evidence for disciplinary action or termination.
- Complying with applicable law.
- Education, training, and development requirements.
- Health administration services.
- Complying with health and safety obligations.
- In connection with your access to NOC premises.

We will only process your Personal Data for the purposes we collected it for or for compatible purposes. If we need to process your Personal Data for an incompatible purpose, we will provide

notice to you and, if required by law, seek your consent. We may process your Personal Data without your knowledge or consent where required by applicable law or regulation.

We may also process your Personal Data for our own legitimate interests, including for the following purposes:

- To prevent fraud.
- To prevent or detect unlawful acts
- To ensure network and information security, including preventing unauthorized access to our computer and electronic communications systems and preventing malicious software distribution.
- To conduct data analytics analyses to review and better understand employee retention and attrition rates.

You will not be subject to decisions based on automated data processing without your prior consent.

Collection and Use of Special Categories of Personal Data and Criminal Conviction Data
The following special categories of Personal Data are considered sensitive under Data Protection Law and may receive special protection:

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Genetic data.
- Biometric data.
- Data concerning health.
- Data concerning sex life or sexual orientation.

Data relating to criminal convictions and offences also receive special protection under Data Protection Law. Criminal convictions data means Personal Data relating to criminal convictions and offences, including Personal Data relating to criminal allegations and proceedings ("Criminal Convictions Data").

We may collect and process the following special categories of Personal Data and Criminal Convictions Data when you voluntarily provide them for the following legitimate business purposes, to carry out our obligations under employment law, for the performance of the employment contract, or as applicable law otherwise permits:

- Trade union membership information where you choose to provide this information.
- Physical or mental health information or disability status to comply with health and safety obligations in the workplace, to make appropriate workplace accommodations, as part of sickness absence monitoring, for the purposes of occupational health and to administer benefits.
- Race or ethnic origin, religious affiliation, health information and sexual orientation to ensure meaningful equal opportunity monitoring and reporting.
- Criminal convictions data may be collected as part of the recruitment process this will be

retained for no longer than 6 months however a record of whether the check was satisfactory or unsatisfactory will be recorded in your employment record.

Where we have a legitimate need to process special categories of Personal Data for purposes not identified above, we will only do so only after providing you with notice and, if required by law, obtaining your prior, express consent.

We will always treat Special Categories of Personal Data and Criminal Convictions Data as confidential, and we will only share such data internally where there is a specific and legitimate purpose for sharing the data. As set out below, we have implemented appropriate physical, technical, and organisational security measures designed to secure your Personal Data against accidental loss and unauthorised access, use, alteration, or disclosure.

We will not use Special Category Personal Data or Criminal Convictions data for new, different or incompatible purposes from those disclosed when it was first obtained unless we have informed you of the new purposes and you have consented (where necessary).

We will only retain special categories of Personal Data for as long as necessary to fulfil the purposes we collected it for, as required to satisfy any legal, accounting, or reporting obligations, or as necessary to resolve disputes.

Data Sharing

We will only disclose your Personal Data to third parties where required by law or to our employees, contractors, designated agents, or third-party service providers who require such information to assist us with administering the employment relationship with you, including third-party service providers who provide services to us or on our behalf. Third-party service providers may include, but are not limited to, payroll processors, benefits administration providers, and data storage or hosting providers. These third-party service providers may be located outside of your home jurisdiction.

We require all our third-party service providers, by written contract, to implement appropriate security measures to protect your Personal Data consistent with our policies and any data security obligations applicable to us as your employer. We do not permit our third-party service providers who process your Personal Data on our behalf to use your Personal Data for their own purposes. We only permit them to process your Personal Data for specified purposes in accordance with our instructions.

We may also disclose your Personal Data for the following additional purposes where permitted or required by applicable law:

- To comply with legal obligations or valid legal processes such as search warrants, or court orders. When we disclose your Personal Data to comply with a legal obligation or legal process, we will take reasonable steps to ensure that we only disclose the minimum Personal Data necessary for the specific purpose and circumstances.
- To protect the rights and property of NOC.
- During emergency situations or where necessary to protect the safety of persons.
- Where the Personal Data is publicly available.
- If a business transfer or change in ownership occurs and the disclosure is necessary to

complete the transaction. In these circumstances, we will limit data sharing to what is absolutely necessary, and we will anonymise the data where possible.

- For additional purposes with your consent (where such consent is required by law).
- Your data could also be shared with employee representatives in the context of collective consultation on a redundancy or merger, if such a situation were to arise. This would be limited to the information needed for the purposes of consultation, such as your name, role and length of service.
- Relevant data (e.g. mobile number) may also be shared for the purposes of the organisation's business continuity plan or serious incident procedures.
- Your data may also be shared for the purposes of audit or compliance purposes including grant funded activity

International transfers of information

We may, on occasion decide to use the services of a supplier outside the European Economic Area (EEA), which means that your personal information is transferred, processed, and stored outside the EEA. You should be aware that, in general, legal protection for personal information in countries outside the EEA may not be equivalent to the level of protection provided in the EEA.

However, we take steps to put in place suitable safeguards to protect your personal information when processed by the supplier such as entering into the International Data Transfer Agreement and Addendum.

Data Security

We have implemented appropriate physical, technical, and organizational security measures designed to secure your Personal Data against accidental loss and unauthorized access, use, alteration, or disclosure. In addition, we limit access to Personal Data to those employees, agents, contractors, and other third parties that have a legitimate business need for such access.

Data Retention

Except as otherwise permitted or required by applicable law or regulation, we will only retain your Personal Data for as long as necessary to fulfill the purposes we collected it for, as required to satisfy any legal, accounting, or reporting obligations, or as necessary to resolve disputes. To determine the appropriate retention period for Personal Data, we consider applicable legal requirements, 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 we process your Personal Data for, and whether we can achieve those purposes through other means. We specify the retention periods for your Personal Data in our data retention policy.

Under some circumstances we may anonymize your Personal Data so that it can no longer be associated with you. We reserve the right to use such anonymous and de-identified data for any legitimate business purpose without further notice to you or your consent. Once you are no longer an employee of the company, we will retain and securely destroy your Personal Data in accordance with our document retention policy and applicable laws and regulations.

Rights of Access, Correction, Erasure, and Objection

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 employment. By law you may have the right to

request access to, correct, and erase the Personal Data that we hold about you, or object to the processing of your Personal Data under certain circumstances. You may also have the right to request that we transfer 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 Data to another party, please contact us at noc_governance@noc.ac.uk. Any such communication must be in writing.

We may request specific information from you to help us confirm your identity and your right to access, and to provide you with the Personal Data that we hold about you or make your requested changes. Applicable law may allow or require us to refuse to provide you with access to some or all of the Personal Data that we hold about you, or we may have destroyed, erased, or made your Personal Data anonymous in accordance with our record retention obligations and practices. If we cannot provide you with access to your Personal Data, we will inform you of the reasons why, subject to any legal or regulatory restrictions.

Right to Withdraw Consent

Where you have provided your consent to the collection, processing, or transfer of your Personal Data, you may have the legal right to withdraw your consent under certain circumstances. To withdraw your consent, if applicable, contact us at noc_governance@noc.ac.uk.

Changes to This Privacy Notice

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 updates. If we would like to use your previously collected Personal Data for different purposes than those we notified you about at the time of collection, we will provide you with notice and, where required by law, seek your consent, before using your Personal Data for a new or unrelated purpose. We may process your Personal Data without your knowledge or consent where required by applicable law or regulation.

Contact Us

If you have any questions about our processing of your Personal Data or would like to make an access or other request, please contact noc_governance@noc.ac.uk.

If you are not happy with the response you receive, then you can raise your concern with the relevant statutory body:

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Alternatively, you can visit the ICO's website https://ico.org.uk/.

Last updated: 04/12/2025