This document reflects UKCEH's commitment to EEDI by ensuring that all Policies, Procedures, and SOPs are reviewed and considered for their impact on the nine protected characteristics. Consistent third-person terminology is used throughout.

**Policy Synopsis: UKCEH Data Protection Policy**

- **Compliance with UK-GDPR and DPA 2018**
  The policy ensures UKCEH meets its legal obligations as a data controller and processor, upholding the six Data Protection Principles, including lawfulness, data minimisation, and integrity.
- **Safeguards for Stakeholders**
  The policy protects the personal data rights of all stakeholders — including staff, students, visitors, research partners and participants — across all research and operational activities.
- **Research and AI-Specific Commitments**
  Special measures are in place for handling research data and AI-related processing, including DPIAs for high risk data, transparency obligations, and safeguards against bias and automated decision-making.
- **Data Security and International Transfers**
  Personal data is protected through technical and organisational controls. Transfers outside the UK/EEA are only permitted under strict legal safeguards, with DPO oversight.
- **Training, Breach Management and Accountability**
  Annual training is mandatory for staff. Any data breaches must be reported within 72 hours, and the policy undergoes annual review with executive oversight.

## 1 Introduction

The UK Centre of Ecology & Hydrology & its Entities (UKCEH) is committed to data protection by default and by design and supports the data protection rights of all stakeholders, including, but not limited to, staff, students, visitors, research partners and participants. This policy sets out the accountability and responsibilities of UKCEH, its staff and its students to comply fully with the provisions of the UK General Data Protection Regulation (UK-GDPR) and the Data Protection Act 2018 ("the DPA") and recognises that handling personal data appropriately and in compliance with data protection legislation protects UKCEH's relationship with all its stakeholders.

UKCEH holds and processes personal data about individuals such as employees, students, fellows and others, defined as 'data subjects' by the law. Such data must only be processed in accordance with the GDPR and the DPA.

UKCEH has appointed a Data Protection Officer (DPO) to monitor and advise on compliance with the GDPR and the DPA.

This policy covers the following areas:

- Purpose of the policy
- Scope of the policy
- Status of the policy
- Responsibilities under the policy
- Data protection by design and default
- Responsibility of management and data users
- Handling of personal data by students
- Data subject rights
- Internal data sharing

- Transfers of personal data outside the EEA
- Data protection training
- Data protection breaches

## 2 Purpose of Policy

This policy sets out the responsibilities of UKCEH, to comply fully with the provisions of GDPR and the DPA. This policy is the framework which everybody processing personal data at UKCEH should follow to ensure compliance with data protection legislation.

## 3 Scope

This policy applies to including, but not limited to, staff, students, visitors, external and internal collaborators, stakeholders and research partners and participants, in all cases where UKCEH is the data controller or a data processor of personal data. The policy applies in these cases regardless of who created the data, where it is held, or the ownership of the equipment used.

## 4 Responsibilities under the Policy

UKCEH as data controller has a corporate responsibility to implement and comply with data protection legislation. In determining the purposes for which, and the way, personal data is processed, UKCEH must adhere to the six Data Protection Principles ("the Principles") as set out in the legislation. These six principles are:

- **Lawfulness, fairness and transparency** - we must process personal data lawfully, fairly and in a transparent manner in relation to the data subject.
- **Purpose limitation** - we must only collect personal data for a specific, explicit and legitimate purpose. You must clearly state what this purpose is, and only collect data for as long as necessary to complete that purpose.
- **Data minimisation** - we must ensure that personal data you process is adequate, relevant and limited to what is necessary in relation to your processing purpose.
- **Accuracy** - we must take every reasonable step to update or remove data that is inaccurate or incomplete. Individuals have the right to request that you erase or rectify erroneous data that relates to them, and you must do so within a month.
- **Storage limitation**- we must delete personal data when they are no longer needed. The timescales in most cases aren't set. They will depend on your business' circumstances and the reasons you collect this data.
- **Integrity and confidentiality** – we must keep personal data safe and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measure

**This section sets out the main requirements for compliance.**

## 5 Data Security

All users of personal data within UKCEH must ensure that personal data are always held securely and are not disclosed to any unauthorised third party either accidentally, negligently or intentionally. The Policies on Data Security and Working with Sensitive Data, be read in conjunction with this Data Protection Policy.

**Privacy Notices**

When UKCEH collects personal data from individuals, the requirement for 'fairness and transparency' must be adhered to. This means that UKCEH must provide data subjects with a 'privacy notice' to let them know how and for what purpose their personal data are processed. Any data processing must be consistent or compatible with that purpose.

**Definition of controller and processor:**

- 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

**Conditions of Processing/Lawfulness**

In order to meet the 'lawfulness' requirement, processing personal data must meet at least one the following conditions:

1. The data subject has given consent.
2. The processing is required due to a contract.
3. It is necessary due to a legal obligation.
4. It is necessary to protect someone's vital interests (i.e. life or death situation).
5. It is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. (As UKCEH is not a public authority, it does not rely on the 'public task' lawful basis. Instead, UKCEH typically uses 'legitimate interests' or consent, depending on the context.)
6. It is necessary for the legitimate interests of the controller or a third party. UKCEH will use this requirement and **NOT Public Task**
7. When processing special category data[1], UKCEH must document its legal basis and justify the necessity of processing. Common lawful bases for UKCEH activities include:
    - Explicit Consent (Article 9(2)(a)) – e.g., voluntary participation in research.
    - Employment, social security & protection (Article 9(2)(b)) – e.g., staff health records.
    - Scientific research, archiving, or statistical purposes (Article 9(2)(j)) – e.g., anonymised research data.

Where possible, special category data should be pseudonymised or anonymised to reduce risk. DPIAs must be conducted for any new processing of special category data.

**Data Retention**

Personal data must be retained only for as long as necessary for the specified processing purposes, in line with UKCEH's **Records Management Policy**. The following retention periods apply:

| Data Type | Retention Period | Rationale |
|---|---|---|
| Employee Records | 7 years after termination | Legal and People Team compliance |
| Research Participant | Varies per project, anonymised if | Research ethics & GDPR |

[1] The term describing a sub-category of personal data that requires heightened data protection measures due to its sensitive and personal nature. Controllers or data owners must satisfy certain requirements before processing special categories of data, such as obtaining data subject consent.

| Data | feasible | compliance |
|---|---|---|
| Financial Transactions | 7 years | HMRC & financial regulations |
| Subject Access Requests | 2 years from resolution | Accountability for data protection requests |

All data retention schedules must be regularly reviewed, and obsolete data must be securely deleted or anonymised.

This applies to all personal data, whether held on UKCEH core systems, local PCs, laptops or mobile devices or held on paper. If the data is no longer required or past its retention period, it must be securely destroyed or deleted. UKCEH's Records Management Policy can be found here and is based on both legal and business requirements.

## 6 Data Protection by Design and Default

Under the GDPR and the DPA, UKCEH has an obligation to consider the impact on data privacy during all processing activities. This includes implementing appropriate technical and organisational measures to minimise the potential negative impact processing can have on the data subjects' privacy.

**Data Protection Impact Assessment**

When considering new high risk processing activities or setting up new procedures or systems that involve personal data, privacy issues must always be considered at the earliest stage and a Data Protection Impact Assessment (DPIA) must be conducted. The DPIA is a mechanism for identifying and examining the impact of new initiatives and putting in place measures to minimise or reduce risks during the design stages of a process and throughout the lifecycle of the initiative. This will ensure that privacy and data protection control requirements are not an after-thought.

This process has two parts, with the first part analysing if there is a requirement for a DPIA. Either part must be signed off by the UKCEH DPO.

A template with guidance for DPIAs can be found here:

**Anonymisation and Pseudonymisation**

Further mechanisms of reducing risks associated with handling personal data are to apply anonymization or pseudonymisation. Wherever possible, personal data must be anonymised or, where that is not possible, pseudonymised.

## 7 Responsibilities of Management and Data Users

All staff and visitors at UKCEH have a responsibility to ensure compliance with the GDPR, the DPA and this policy, and to develop and encourage good information handling practices within their areas of responsibility. All users of personal data within UKCEH have a responsibility to ensure that they process the data in accordance with the Principles and the other conditions set down in the legislation.

The DPO will perform periodic audits to ensure compliance with this policy and the legislation. This will also be audits during standard project audits.

## 8 Handling Personal Data in Research

Before collecting or processing personal data in research, UKCEH researchers must:

- Conduct a **Data Protection Impact Assessment (DPIA)** to assess risks.
- Provide a **Participant Information Sheet** explaining how data will be used.
- Obtain **informed consent** where required.
- Ensure **withdrawal procedures** are in place where consent is the basis for processing.
- Use **pseudonymisation/anonymisation** where possible to minimise risks.

If data subjects request withdrawal, UKCEH must assess if the data can be deleted without affecting research validity. Where research exemptions apply under **DPA 2018 Schedule 2**, UKCEH will document this justification.

## 9 Data Subject Rights

The GDPR and the DPA contain eight data subject rights UKCEH must comply with – the rights to information (see Privacy Notices), subject access, to rectification, to object, to erasure, to portability, to restrict processing and in relation to automated decision-making and profiling. These rights can be restricted for personal data used in research.

**Subject Access Requests and the right to data portability**

Individuals have the right to request to see or receive copies of any information UKCEH holds about them, and in certain circumstances to have that data provided in a structured, commonly used and machine-readable format so it can be forwarded to another data controller. UKCEH must respond to these requests within four weeks. It is a personal criminal offence to delete relevant personal data after a subject access request has been received.

**Right to erasure, to restrict processing, to rectification and to object**

In certain circumstances data subjects have the right to have their data erased. This only applies:

- where the data is no longer required for the purpose for which it was originally collected, or
- where the data subject withdraws consent, or
- where the data is being processed unlawfully.

In some circumstances, data subjects may not wish to have their data erased but rather have any further processing restricted.

If personal data is inaccurate, data subjects have the right to require UKCEH to rectify inaccuracies. In some circumstances, if personal data are incomplete, the data subject can also require the controller to complete the data, or to record a supplementary statement.

Data subjects have the right to object to specific types of processing such as processing for research or statistical purposes. The data subject needs to demonstrate grounds for objecting to the processing relating to their particular situation.

Individuals receiving any of these requests should not act to respond but instead should contact the Data Protection Officer immediately.

**Rights in relation to automated decision making and profiling**

UKCEH does not engage in automated decision-making that produces legal or similarly significant effects on individuals. If automated processing is introduced in future, UKCEH will:

- Ensure **human oversight** is embedded in decision-making.
- Provide individuals with the right to challenge automated decisions.
- Conduct a **DPIA before implementation** to assess risks.

Staff must seek **DPO approval** before implementing automated processing.

## 10 Data Sharing

When personal data is transferred internally, the recipient must only process the data in a manner consistent with the original purpose for which the data was collected. If personal data is shared internally for a new and different purpose, a new privacy notice will need to be provided to the UKCEH staff to whom this data relates.

When personal data is transferred externally, a legal basis must be determined and a data sharing agreement between UKCEH and the third party must be signed, unless disclosure is required by law, such as certain requests from the Department for Work and Pensions or Inland Revenue, or the third party requires the data for law enforcement purposes. Where data sharing agreements are in place, these must be recorded centrally by the DPO or Contracts

## 11 Transfers of Personal Data outside the EEA

Personal data can only be transferred out of the European Economic Area when there are safeguards in place to ensure an adequate level of protection for the data.

*For transfers of personal data outside the UK or EEA, UKCEH must ensure appropriate safeguards are in place. Transfers may only occur under one of the following conditions:*

- The receiving country has an adequacy decision from the UK or the EU.
- Standard Contractual Clauses (SCCs) or the UK International Data Transfer Agreement (IDTA) are used.
- Binding Corporate Rules (BCRs) are in place where applicable.
- An exception under Article 49 UK-GDPR applies, such as explicit consent or contract necessity.

Before transferring personal data internationally, staff must seek Data Protection Officer (DPO) approval and confirm that safeguards meet UK-GDPR requirements.

## 12 Use of Artificial Intelligence (AI) in Data Processing

CEH recognises the growing use of Artificial Intelligence (AI) in scientific research, decision-making, and administrative operations. Where AI systems process personal data, UKCEH is committed to ensuring full compliance with the UK General Data Protection Regulation (UK-GDPR) and the Data Protection Act 2018, and to protecting the rights and interests of all stakeholders — including, but not limited to, staff, students, visitors, research partners, and research participants.

When AI is used in any context involving personal data:

- **Lawfulness and Transparency**
  Personal data must be processed lawfully, fairly, and transparently. Individuals must be informed if their data is used in AI-driven systems, including information about the nature, scope, and logic of automated processes.

- **Data Protection Impact Assessments (DPIAs)**
  A DPIA must be conducted before implementing any high risk AI system that involves the processing of personal or special category data. The DPIA must specifically assess risks related to profiling, data accuracy, bias, and potential discrimination.

- **Human Oversight**
  Fully automated decision-making which has legal or similarly significant effects on individuals will not be undertaken without meaningful human involvement. Where AI assists in decision-making, human review and accountability must be maintained.

- **Fairness and Bias Mitigation**
  UKCEH will take reasonable steps to ensure that AI systems are free from unfair bias or discrimination, especially when used in HR, funding decisions, or research evaluation. Any use of training data must be appropriate, representative, and auditable.

- **Data Subject Rights**
  Individuals retain all rights under UK-GDPR, including the rights to object, to access their data, to request correction, and to challenge decisions made (in whole or in part) using AI systems.

- **Security and Confidentiality**
  AI systems must be deployed with appropriate technical and organisational safeguards, particularly when they process sensitive or special category data.

- **DPO Oversight**
  All planned or proposed uses of AI systems involving personal data must be reviewed and approved by the Data Protection Officer (DPO) prior to deployment

## 13 Data Protection Training

UKCEH Executive Committee agreed that it should be mandatory for all staff members to annually complete the current Data Protection Training eLearning module or refresher.

## 14 Data Protection Breaches

UKCEH is responsible for ensuring appropriate and proportionate security for the personal data that it holds. This includes protecting the data against unauthorised or unlawful processing and against accidental loss, destruction or damage of the data. UKCEH makes every effort to avoid data protection incidents, however, it is possible that mistakes will occur on occasions. Examples of personal data incidents might occur through:

- Loss or theft of data or equipment
- Ineffective access controls allowing unauthorised use
- Equipment failure
- Unauthorised disclosure (e.g. email sent to the incorrect recipient)
- Human error
- Hacking attack

Any data protection incident must be brought to the attention of UKCEH's Data Protection Officer who will investigate and decide if the incident constitutes a data protection breach. If a reportable data protection breach occurs, UKCEH is required to notify the Information Commissioner's Office as soon as possible, and not later than 72 hours after becoming aware of it. Any member of UKCEH community who encounters something they believe may be a data protection incident must report it immediately to UKCEH Data Protection

## 15 Review of the DPIA's

The DPIA's are a live document and will be reviewed after a significant change or every six months. The Executive Committee will receive an annual GDPR report.

## 16 Policy Review and Version Control

This policy will be reviewed annually, or earlier if legislative changes occur. Changes will be documented in the Policy Amendment History section. Any amendments will be approved by the Executive Committee and Data Protection Officer.

**END OF DOCUMENT**