Data Protection Policy

The Institution of Environmental Sciences (IES) is committed to being fully compliant with applicable UK and EU data protection legislation in respect of personal data, and to safeguard the rights and freedoms of persons whose information we collect, pursuant to the General Data Protection Regulation (GDPR).

This policy applies to all employees, trustees, contractors, subcontractors, committee members, volunteers and any others who receive confidential or restricted information during their dealings with us.

Objectives

The objectives for our Data Protection Policy (DPP) are to:

1. safeguard personnel, member and other stakeholder interests;
2. ensure compliance with applicable obligations (statutory, regulatory, contractual and/or professional)
3. meet our personal data obligations in relation to how personal information is managed;
4. support our objectives; and
5. set appropriate systems and controls according to our risk appetite.

GDPR background

The purpose of GDPR is to ensure the rights and freedoms of living individuals, and to protect their personal data by ensuring that it is never processed without their knowledge and, when possible, their consent.

Definitions

Child	Anyone under the age of 16.
Data controller	A natural or legal person, whether public authority, agency or other body, which, individually or jointly with others, is in charge of ascertaining the purposes and means by which personal data shall be processed.
Data processor	A natural or legal person responsible for processing personal data on behalf of a controller.
Data subject	Any living person who is the subject of personal data (see below for the definition of personal data) held by an organisation. A data subject must be identifiable by name, ID, address, online identifier or other factors such as physical, physiological, genetic, economic or social.
Personal data	Any information relating to a data subject.
Personal data breach	A security breach which results in the disclosure, alteration, destruction or loss of personal data, as well as unauthorised access to personal data that is stored, transmitted or processed by any other means, whether accidentally or unlawfully.
Processing	Any action taken in relation to personal data, including but not limited to collection, adaptation or alteration, recording, storage, retrieval, consultation, use, disclosure, dissemination, combination or deletion, whether by automated means or otherwise.
Profiling	Any form of personal data processing that is automated, with the intention of assessing personal aspects of a data subject or analysing a data subject's employment performance, economic status, whereabouts, health, personal preferences and behaviour. The data subject has a right to object to profiling and a right to be informed of the fact that profiling is taking place, as well as the intended outcome(s) of the profiling.
Third party	A natural or legal person, other than the data subject, who is authorised to process personal data, whether a public authority, agency or other body controller, processor or any other person(s) under the direct authority of the Controller or Processor.

Practice

We shall ensure compliance with data protection legislation and good practice by:

1. processing personal information only when necessary for organisational purposes;
2. ensuring the least possible amount of personal data is collected, for specified, explicit and legitimate reasons;
3. only using personal data obtained for specific purposes in relation to that purpose;
4. ensuring that personal data is not processed unduly and there is a clear lawful basis for processing;
5. informing individuals of how their personal data is, or will be, used and by whom, in a transparent, easily accessible and clear manner;
6. processing only pertinent and adequate personal data;
7. processing personal data in a lawful and fair manner, following principles laid out in our Fair Processing Procedures;
8. keeping a record of the categories of personal data processed;
9. taking reasonable steps to keep personal data accurate and up-to-date;
10. retaining personal data no longer than required by statute, regulatory body, or for organisational purposes in line with our Retention & Archiving Policy;
11. ensuring personal data kept beyond the processing date is either deleted, encrypted, pseudonymised or put beyond use and kept to an absolute minimum to protect the data subject's identity;
12. giving individuals the right of subject access and other individual rights pertaining to personal data;
13. taking reasonable steps to ensure personal data is maintained securely;
14. only transferring personal data outside of the EU in circumstances where it is appropriately secured;
15. applying statutory exemptions, where appropriate; and
16. identifying internal and external individuals who have access to data and assuring they are responsible and accountable for upholding the data protection policies.

Notification

We have identified the personal data that we process and have recorded it in our Data Inventory which is reviewed on an annual basis by our Data Protection Officer (DPO). Any personal data breaches will be reported to relevant regulatory authority. The data subject will be informed of a data breach when it is likely that the breach will have an adverse effect on their privacy or personal data. The DPO retains a copy of any notifications we make to the Information Commissioner's Office (ICO).

Breaches of the DPP are dealt with according to the IES's Disciplinary Procedures. If the breach could amount to a criminal offence, the matter shall be referred to the relevant authorities.

Third parties

Third parties working with or for us, who have or may have access to personal data, are required to read, understand and fully comply with this policy. All these third parties are required to enter into a data confidentiality agreement prior to accessing personal data. The data protection obligations imposed by the confidentiality agreement are equally onerous as those to which we have agreed to comply. We have the right to audit any personal data accessed by third parties pursuant to the confidentiality agreement.

Responsibilities under GDPR

The IES is a Data Controller pursuant to GDPR.

Accountability

We are responsible both for ensuring overall compliance with GDPR and for demonstrating that each of our processes are compliant with GDPR requirements. To this extent, we:

- maintain all relevant documentation regarding its processes and operations;
- implement proportionate security measures;
- carry out Privacy Impact Assessments;
- comply with prior notification requirements;
- seek the approval of relevant regulatory bodies; and
- appoint a DPO.

The Data Protection Officer

The DPO oversees the management of personal data, compliance with GDPR requirements and promotion of good practice. The DPO reports to the IES Council (its governing body) and is accountable for the development and implementation of the DPP and for day-to-day compliance, both in terms of security and risk management. In addition, the DPO is responsible for ensuring the IES and its employees and contractors are GDPR compliant, and acts as their first point of contact for guidance in relation to data protection.

The DPO ensures that that personal data which is superfluous, and not necessarily required for the purpose(s) for which it is obtained, is not collected. They approve all data collection forms and carry out an annual review of methods of data collection, checking that they are still appropriate, relevant and not excessive. They securely delete or destroy any personal data that does not meet that criteria.

It is not only the DPO who is responsible for data protection; all IES employees, volunteers, and sub-contractors who process personal data are responsible for ensuring compliance with data protection laws. Appropriate training is given to staff and contractors to help them with this. Employees, volunteers and sub-contractors of the IES are also personally responsible for ensuring that personal data they provide to the IES is accurate and up-to-date.

Risk Assessment

The DPO makes sure that appropriate controls are in place to ensure that the risk level associated with personal data processing is kept to an acceptable level, as per GDPR requirements and our risk appetite.

We carry out assessments of the personal data processing undertaken by organisations on our behalf and manage any identified risks to mitigate the likelihood of potential non-compliance with this policy.

Where personal data processing is carried out using new technologies, when we launch a new data sharing initiative, or when personal data is used for new purposes, we engage in a risk assessment of the potential impact, known as a Privacy Impact Assessment (PIA). If the outcome points to a high risk that data processing could result in distress or may cause damage to data subjects, the DPO decides whether we ought to proceed. The DPO may escalate the matter to the regulatory authority if significant concerns are identified.

Consent

Consent to the processing of personal data by the data subject must be:

- freely given and never under duress, when the data subject is in an unfit state of mind or provided on the basis of misleading or false information;
- explicit and specific;
- a clear and unambiguous indication of the wishes of the data subject, provided either in a statement or by unambiguous affirmative action;
- informed;
- demonstrated by active communication between the data controller and the data subject and never inferred or implied by omission or a lack of response to communication; and

- in relation to sensitive data, consent may only be provided in writing, unless there is an alternative legitimate basis for the processing of personal data.

Parental Consent

We only process personal data of a child upon receipt of consent from their parent or legal custodian.

Data Protection Principles

The data subject will always be provided with the following information:

1. identity and contact details of our DPO;
2. purpose or purposes and lawful basis of processing;
3. length of time for which data shall be stored;
4. confirmation of the existence of the rights to request access, rectify, erase or raise an objection to the processing of personal data;
5. categories of personal data;
6. recipients of personal data, if applicable;
7. if we intend to transfer personal data to a third country and the levels of data protection provided; and
8. any further information required by the data subject to ensure fair and lawful processing.

Employees

We employ several lawful bases for processing employees' details, including contract, legal obligation, consent and legitimate interests. We comply with the principles of proportionality and subsidiarity, auditing whether personal data collected is necessary and outweighs the general privacy rights that employees have in the workplace. Employees are notified of their rights in our Employee Handbook and their obligations in our Procedures Manual.

Other Data Subjects

In most cases, we use consent as a lawful basis for collecting and processing data. When a data subject has indicated their wishes, we reserve the right to make use of that data. We only use data for the purpose for which it was collected.

When using consent as a condition to process data, we obtain consent in accordance with the procedures outlined in our Fair Processing and Data Protection Principles. Consent is a positive action on behalf of the data subject having read a clear, transparent and unambiguous privacy notice. It is not always a box that is ticked, it could be the completion of a form, or the supply of contact information. According to the Privacy and Electronic Communications Regulations (PECR), consent does not have to be explicit, so we use our judgement to decide how to obtain consent in different circumstances. We always uphold the rights and freedoms of data subjects by always making it as easy to opt out as it was to opt in.

Information Security Policy

The processing of personal data is always carried out in a secure manner. Security controls ensure that risks to personal data are mitigated as much as possible to reduce potential for damage or distress to data subjects. Procedures for staff and committee members are laid out in our Security Policy & Procedures. All employees are personally responsible for keeping secure personal data held by the IES.

Accessing Personal Data

Access to personal data is only granted to those who need it and only according to the principles of our Information Security Policy & Procedures. Under no circumstances is personal data disclosed to a third party, unless authorisation has been provided via a confidentiality agreement or consent has been given by the data subject.

Adequacy of Transfer

Safeguards and exceptions are in place to ensure data is not transferred to a country outside of the EU, unless either we have:

1. fully assessed the adequacy of the transfer by determining:
   - the nature of the personal data to be transferred;
   - the country of origin and country of intended destination;
   - the nature and duration of the personal data use;
   - the legislative framework, codes of practice and international obligations of the data subject's country of residence; and
   - the security measures to be implemented in the country of intended destination in relation to the personal data;
2. Received permission or approval of model contract clauses from the relevant regulatory body to implement approved binding corporate rules in relation to personal data transfer outside of the EU; or
3. Satisfied one of the following preconditions:
   - explicit consent has been provided by a fully informed data subject who has been made aware of all possible risks involved;
   - personal data transfer is a prerequisite to the performance of a pre-existing contract between the data controller and the data subject, or when the data subject requests that pre-contractual measures are implemented;
   - personal data transfer is a prerequisite to the conclusion or performance of a pre-existing contract between the data controller and another person, whether natural or legal, if it is in the interest of the data subject;
   - personal data transfer is in the public interest or is required for the creation, exercise or defence of legal claims;
   - the data subject is not capable of giving consent, whether due to physical or legal limitations or restrictions. In these cases, the data transfer must be necessary for the protection of the key interests of the data subject or of other persons; or
   - the personal data transfer is made from an approved register, confirmed by EU or Member State law as having the intention of providing public information and which is open to consultation by the public or by an individual demonstrating a legitimate interest.

The Rights of Data Subjects

Data subjects enjoy the following rights in relation to personal data that is processed and recorded, to:

1. make access requests in respect of personal data that is held and disclosed;
2. refuse personal data processing when to do so is likely to result in damage or distress;
3. refuse personal data processing when it is for direct marketing purposes;
4. be informed about the functioning of any decision-making processes that are automated which are likely to have a significant effect on the data subject;
5. solely be subject to any automated decision-making process;
6. claim damages should they suffer any loss due to a breach of the provisions of the GDPR;
7. take appropriate action in respect of the following: the rectification, blocking and erasure of personal data, as well as the destruction of any inaccurate personal data;
8. request that the ICO carry out an assessment as to whether any of the provisions of the GDPR have been breached;
9. be provided with personal data in a format that is structured, commonly used and machine-readable;
10. request that their personal data is sent to another data controller; and
11. refuse automated profiling without prior approval.

Data Access Rights

Data subjects have the right to access all personal data in relation to them held by us, whether as manual records or electronic. To do so, a data subject should submit a Subject Access Request, as outlined in the Subject Access Request Policy.

Disclosure of Data

We take appropriate steps to ensure that no personal data is disclosed to unauthorised third parties. This includes friends and family members of the data subject, governmental bodies and, in special circumstances, even the police. All employees attend specific training to learn how to exercise due caution when requested to disclose personal data to a third party.

GDPR permits disclosure without consent of the data subject under certain circumstances, in the interest of:

- safeguarding national security;
- crime prevention and detection, including the apprehension and prosecution of offenders;
- assessing or collecting a tax duty;
- discharging various regulatory functions, including health and safety;
- preventing serious harm occurring to a third party; and
- protecting the vital interests of the data subject i.e. only in a life and death situation.

The DPO is responsible for handling all requests for the provision of data for these reasons. Authorisation by the DPO is only be granted with support of appropriate documentation.

Data Retention and Disposal

Once a member, employee, contractor or other stakeholder leaves or ceases business with the IES, it may no longer be necessary to retain all, or any, personal data related to that individual. Some data may be kept in line with our Retention & Archiving Policy. Data will be disposed of accordingly, ensuring that the rights and freedoms of data subjects.

All deletion of personal data must be carried out in accordance with our Retention & Archiving Policy. Manual records which have passed their retention date are shredded, and any removable computer media (such as hard drives or USBs) are destroyed as outlined in our Information Security Policy & Procedures.

Under GDPR, we process personal data for archiving purposes beyond the stated retention period when doing so is in the public interest, or for historical, scientific or statistical purposes. In such circumstances, we ensure archiving does not contravene the rights and freedoms of data subjects and that appropriate safeguards have been put in place, such as data minimisation, pseudonymisation or encryption.

Complaints

Complaints about our processing of personal data may be lodged by a data subject by contacting the DPO and providing details of the complaint.

Complaints may also be made by a data subject directly to the relevant regulatory body:

Information Commissioner's Office (ICO) | https://ico.org.uk/concerns | +44 (0)303 123 1113

Complaints in relation to how a complaint has been handled, and any appeals following the submission of a complaint, shall be dealt with by the IES Council (governing body).

Change History Record

Issue	Description of Change	Approval	Date of Issue