

*Ireland's Environmental Education
and Youth Organisation*



ECO-UNESCO

Data Protection Policy

Version 2018.05

Our relationship to personal information

ECO-UNESCO is a data controller for the purposes of Data Protection legislation in the majority of cases where we process personal information.

Under certain circumstances ECO-UNESCO may operate as a Data Processor. For example another organisation may engage us to provide training to their employees or participants. In this scenario, they are the Data Controller and ECO-UNESCO the Data Processor

Finally, there are times when ECO-UNESCO may act as a Joint Data Controller, whereby responsibility with another organisation is shared equally due to the nature of the relationship.

Being a data controller carries with it serious legal responsibilities and all data controllers must comply with certain important rules about how they collect and use personal information.

As a Data Controller, ECO-UNESCO is committed to protecting the personal information in our progression. We aim to adhere to the 7 key principles said out in the EU General Data Protection Regulations:

1. Lawful, fair and transparent processing
2. Purpose limitation
3. Data minimisation
4. Data accuracy
5. Storage limitation
6. Security, integrity and confidentiality
7. Accountability

We will only process personal information once we are satisfied that our processing meets one of the following legal basis:

1. Consent
2. Fulfilment of a Contract
3. Legal obligation
4. Vital interests of an individual
5. Public task
6. Legitimate interest

In relation to Sensitive Personal Information, we will only process this information once one or more of the following criteria have been met:

1. Consent
2. Carrying out obligations and exercising specific rights in the field of employment and social protection
3. To protect the vital interest of the data subject where they are physically or legally incapable to giving consent
4. Legitimate activities of a not for profit body with a philosophical aim
5. The data is manifestly made public by the data subject
6. Necessary for the establishment, exercise or defence of a legal claim, or by court order
7. Public interest
8. For the assessment of the working capacity of an employee
9. Public Health
10. Archiving in the public interest

ECO-UNESCO will adopt the same high standards where we operate as a Data Processor. However, the exact criteria which will be applied will be defined by the Data Controller any such instance.

Our commitment to Privacy

ECO-UNESCO's Data Protection Policies are designed to comply with the following legislation:

- The Data Protection Act 1988
- The Data Protection (Amendment) Act 2003
- The General Data Protection Regulation (2018)
- The Data Protection Act (2018 currently in Bill form)

ECO-UNESCO collects and processes personal data relating to its employees in the course of business in a variety of circumstances, e.g. recruitment, training, payment, performance reviews, and to protect the legitimate interests of ECO-UNESCO. It also collects and processes personal data relating to its members, participants, students and employees of partner organisations in the course of business in a variety of circumstances.

This policy covers any individual about whom this organisation processes data. This may include current and former employees, current & former members, programme participants, current & former volunteers, interns, trainees and employees of partner organisations with whom we work. Processing of data includes: collecting; recording; storing; altering; disclosing; destroying; and blocking.

Employees Data: Personal data kept by this organisation shall normally be stored in the employee's personnel file or electronic database.

Participant, Member and Partner Data: Participant, member and partner data kept by ECO-UNESCO is stored securely on our Salesforce CRM system with restricted access to highly sensitive data, such as PPS numbers and medical information. Additional information may be held on our email system or document management system.

ECO-UNESCO will ensure that only authorised personnel have access to an individual's personal information. ECO-UNESCO have implemented appropriate security measures in place to protect against unauthorised access.

As participants and young people taking part in programmes with ECO-UNESCO will often be under the age of eighteen, parental consent will always be sought in relation to the data of minors.

Collection and storage of data

ECO-UNESCO processes certain data relevant to the nature of the employment regarding its employees and, where necessary, to protect its legitimate business interests.

ECO-UNESCO processes certain data relevant to the purpose of the organisation, i.e. the delivery of our mission to protect the natural environment and empower young people. In practice this will involve the delivery of programmes, workshops, and events to participants in conjunction with partner organisations.

ECO-UNESCO processes certain data relevant to the running of an organisation, i.e. the engagement and management of suppliers and customers.

We will ensure that personal data will be processed in accordance with the principles of data protection, as described in the Data Protection Acts 1988 and 2003.

Personal data is normally obtained directly from the individual concerned. In certain circumstances, it will, however, be necessary to obtain data from third parties, e.g., references from previous employers, participant information from a partner organisation. As it is relevant to the nature of this organisations work, and required under law, ECO-UNESCO will make an application to the Garda Vetting Bureau for Garda clearance of an employee or volunteer/intern, through the National Youth Council of Ireland (NYCI).

Personal data collected by ECO-UNESCO is used solely for purpose for which it was collected. Where there is a need to collect or utilise data for another purpose, ECO-UNESCO shall inform the data subject of this. In cases where it is appropriate to get the data subject's consent to such processing, ECO-UNESCO will do so.

ECO-UNESCO is under legal obligation to keep certain data for a specified period of time. In addition, ECO-UNESCO will need to keep personnel data for a period of time in order to protect its legitimate interests.

Security and disclosure of data

ECO-UNESCO will take all reasonable steps to ensure that appropriate security measures are in place to protect the confidentiality of both electronic and manual data. Security measures will be reviewed from time to time, having regard to the technology available, the cost and the risk of unauthorised access. ECO-UNESCO Employees, volunteers and interns must implement all organisational security policies and procedures, e.g., use of computer passwords, locking filing cabinets. Personal data will only be processed for the purposes declared at the time of collection and, in general, will not be disclosed to third parties, except where required or authorised by law or with the agreement of the Data Subject.

Employees may have access to a certain amount of personal data relating to colleagues, customers, participants and other third parties. All employees must play their part in ensuring its confidentiality. They must adhere to the data protection principles and must not disclose such data, except where necessary in the course of their employment, or in accordance with law. They must not remove or destroy personal data except for lawful reasons.

Any breach of the data protection principles is a serious matter and may lead to disciplinary action up to and including dismissal. If employees are in any doubt regarding their obligations, they should contact the National Director.

Medical data

ECO-UNESCO may carry out pre-employment medicals as part of the recruitment process. This data will be retained by ECO-UNESCO. Occasionally, it may be necessary to refer employees to ECO-UNESCO's doctor for a medical opinion and all employees are required by their contract of employment to attend.

ECO-UNESCO may, in the interest of the Health & Safety of participants in our programmes, request that participants make a voluntary declaration of any medical issues. This data will be treated in complete confidence and not disclosed to any 3rd party

ECO-UNESCO may receive certain medical information, which will be stored in a secure manner with the utmost regard for the confidentiality of the document. ECO-UNESCO does not retain medical reports on job applicants who do not become employees, or for programme participants, for longer than is necessary.

Employees are required to submit sick certificates in accordance with the sick leave policy. These will be stored by ECO-UNESCO, having the utmost regard for their confidentiality. In attaining a sick certificate, employees are advised to request that the doctor providing the certificate only indicate that they are medically unfit for work and to indicate an expected return to work date. Further medical information is not required.

Electronic Devices

In the case of electronic devices owned by ECO-UNESCO, ECO-UNESCO has the right to, and will, inspect, monitor, and review employee use of employer provided or paid for technology, including but not limited to e-mail, Internet, and cell phone records – including text messages.

ECO-UNESCO will restrict access to all electronic devices owned by the organisation with a view to preventing unauthorised access. These measures will include;

- requiring passwords/PIN access controls
- password complexity policies
- user privilege policies
- network access restrictions
- encryption
- the installation of security software

And any other measure the organisation deems relevant.

Additionally, ECO-UNESCO will employ measures to monitor network traffic on its network (including Virtual Private Networks), and software to monitor file and email access.

ECO-UNESCO's systems will retain logs of any such activity, and these will be reviewed as necessary to ensure the integrity of our systems.

The use of technology in any way that violates the law or company policies is strictly prohibited.

Data Protection Manager

The National Director oversees data protection in the organisation. He/she delegates responsibility for this to the Operations & Development Manager who acts as the Data Protection Manager for ECO-UNESCO. He/she bears overall responsibility for ensuring compliance with data protection legislation, including;

- Addressing Subject Access Requests
- Carrying out Data Privacy Impact Assessments (where necessary)
- Addressing Right to Erasure Requests
- Addressing Right to Rectification Requests

All employees must co-operate with the Data Protection Manager when carrying out his or her duties.

The Data Protection Manager is also available to answer queries or deal with employees' concerns about data protection.

Transfer of Personal Information outside of the EEA

It may be necessary in the course of business for ECO UNESCO to transfer Personal Data to third party service providers in countries outside of the European Economic Area. When this is required, the Organisation will take steps to ensure that the data has the same level of protection as it does inside of the European Economic Area. ECO-UNESCO will only transfer the data to third parties that provide an "adequate level" of protection as defined by the European Commission on the basis of Article 45 of [Regulation \(EU\) 2016/679](#). Data that is transferred to a company in the United States which has signed up to the 'Safe Harbour' is permissible

Subject Access Requests

All individuals (Data Subjects), be they employees, participants, funders, or others, have a right to request a copy of all data ECO-UNESCO holds about them.

Data Subjects may initiate this request through a variety of means, including Social Media, phone or directly to a member of staff. All requests must be treated seriously, and the Data Subject should be directed to submit a formal request either:

| | |
|--|--|
| In writing to: Data Protection Manager ECO-UNESCO 9 Burgh Quay Dublin 2 | By email to: dataprotection@ecounesco.ie |
|--|--|

ECO-UNESCO will respond to all Subject Access Requests within 30 days of the initial request. Should a request be particularly complicated and is likely to require additional time beyond 30 days to complete, the Data Subject will be informed of this and the reasons why.

The Data Protection Manager will respond to the individual making the request to verify their identity, and to seek relevant criteria on which the search of our database and filing systems will be carried out. There is no charge to the Data Subject for making a Subject Access Request. However, repeated requests in a short period of time, or which can be described as "manifestly unfounded or excessive" may incur charges.

Data Subjects are only entitled to access a copy of their own data held by ECO-UNESCO. Data relating to other individuals, or confidential organisational information, will be redacted from the formal response to the request.

- The purposes of the processing
- The categories of personal data concerned
- To whom the personal data has been or will be disclosed
- Whether the data will be or has been transferred outside of the EU
- The period for which the data will be stored, or the criteria to be used to determine retention periods
- The right to make a complaint to the DPC
- The right to request rectification or deletion of the personal data
- Whether the data has been subject to automated decision making

Data that is classified as the opinion of another person, will be provided unless it was given on the understanding that it will be treated confidentially. Employees who express opinions about other Employees in the course of their Employment should bear in mind that their opinion may be disclosed in an access request, e.g. performance appraisals.

A Data Subject who is dissatisfied with the outcome of a Subject Access Request has the right to forward the matter to the Data Protection Commissioner.

A record of all Subject Access Requests shall be kept for a period of 2 years.

Right to Erasure

All Data Subjects about whom ECO-UNESCO hold personal information have the right to request that such information be erased, so long as one or more of the following criteria apply:

- the personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- the data subject withdraws consent on which the processing is based according to point (a) of [Article 6\(1\)](#), or point (a) of [Article 9\(2\)](#), and where there is no other legal ground for the processing;
- the data subject objects to the processing pursuant to [Article 21\(1\)](#) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to [Article 21\(2\)](#);
- the personal data has been unlawfully processed;
- the personal data has to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
- the personal data have been collected in relation to the offer of information society services referred to in [Article 8\(1\)](#).

Data Subject's wishing to have personal information erased should be directed to submit a formal request either:

| | |
|--|--|
| In writing to: Data Protection Manager ECO-UNESCO 9 Burgh Quay Dublin 2 | By email to: dataprotection@ecounesco.ie |
|--|--|

The Data Protection Manager will discuss the request with the Data Subject, verify their identity, and clarify the data to which the request relates. The Data Protection Manager will then assess the legal basis upon which the information is held. Provided the request is compliant with the criteria above, and will not cause ECO-UNESCO to become in breach of existing contracts, obligations or laws, the data shall be deleted and notification made to the Data Subject. In the event that ECO-UNESCO find that there is a legal basis upon which the data should continue to be held, the Data Protection Manager will confirm this finding to the Data Subject.

A Data Subject who is dissatisfied with the outcome of a Right to Erasure Request has the right to forward the matter to the Data Protection Commissioner.

Right to Rectification

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

All Data Subjects about whom ECO-UNESCO hold personal information have the right for this information to be accurate and upto date. In the event that data is incorrect, they have the right to request ECO-UNESCO update such information to be true and accurate.

Where a Data Subject invokes their right to rectification, ECO-UNESCO will verify which data is in need of correction and update such information as quickly as is reasonably practicable.

Individuals wishing to have their personal information updated or corrected should be directed to submit a formal request either:

| | |
|--|--|
| In writing to: Data Protection Manager ECO-UNESCO 9 Burgh Quay Dublin 2 | By email to: dataprotection@ecounesco.ie |
|--|--|

The Data Protection Manager will discuss the request with the Data Subject, verify their identity, verify the inaccurate or incomplete information and make the necessary amendments to our database or files.

Right to Restrict Processing

All Data Subjects about whom ECO-UNESCO hold personal information have the right to restrict, or limit the processing of that information, either temporarily or permanently. For clarity, processing of data can include anything from performing an analysis of the data to deleting that data.

Individuals wishing to have the processing of their personal information restricted should be directed to submit a formal request either:

| | |
|--|---|
| In writing to: Data Protection Manager ECO-UNESCO 9 Burgh Quay Dublin 2 | By email to: dataprotection@ecounesco.ie |
|--|---|

The Data Protection Manager will discuss the request with the Data Subject, verify their identity, verify the data and processing in question and put the necessary restrictions in place, either temporarily or permanently.

Social Media

ECO-UNESCO is active on most major social networks in order to communicate with our participants, supporters and partners, and to promote our work.

ECO-UNESCO recognise that by its very nature, social media is centred around the sharing of personal information.

To protect the right to privacy of any individual with whom ECO-UNESCO interact on social media, the following rules must be followed:

- ECO-UNESCO staff or interns who may have cause to interact with an individual through social media, should only do so through an official ECO-UNESCO account. Personal accounts should never be used.
- ECO-UNESCO staff or interns should never seek to connect (like, friend or follow etc) with any individual they interact with through ECO-UNESCO's presence on social media on their personal accounts.
- ECO-UNESCO staff or interns should never retain any personal information (including images) they are exposed to through ECO-UNESCO's social media profiles.
- ECO-UNESCO staff or interns should never seek to link an individual's social media profiles to other information they may possess (e.g. associating a Facebook profile with an email received) unless such connection is suggested, or consented to, by the individual

Data Breach Policy

In the event that a Data Breach occurs, ECO-UNESCO is committed to both adhering to its obligations under law, but also to protecting the individual(s) involved.

As soon as any ECO-UNESCO employee, volunteer or intern have reason to believe a data breach has occurred, they must immediately (even over evenings or weekends) contact the Data Protection Manager (in the first instance) or the National Director.

An investigation will be carried out to ascertain what has happened. In the event that a breach is confirmed to have occurred, ECO-UNESCO will make a report to the Office of the Data Protection Commissioner within 72 hours.

During this time the Chairperson of the Board will be informed, in addition to our legal advisors and any other counsel whose support is deemed necessary.

Where the breach is deemed to have included personal information that would pose a risk to the data subject's involved, ECO-UNESCO will endeavour to contact the data subjects in question to inform them of the breach.

Use of Images Policy

In carrying out its work, ECO-UNESCO will have cause to take and retain photographic images of the programmes, workshops and events we run.

Inevitably these images will contain (biometric) personal information of the individuals featured within them.

At any events where images of participants will be captured, ECO-UNESCO will inform those in attendance that photographs are being taken (and for what purposes, including where they may be utilised) and provide a method for individuals to indicate their consent (or lack thereof), to their images being taken.

In the interests of practicality, ECO-UNESCO will adhere to an individual's wishes regarding photography where their presence in the photo is deemed to be such that they can be considered the focus of the image (e.g. an individual, or group, taking part in a workshop where faces are clearly visible and in focus).

Images where an individual is in the periphery, only partially visible, or otherwise not the focus, to the point where their identity cannot be easily ascertained by a person to whom they are not known, shall be treated as not containing any personally identifiable information and therefore not subject to an individual's consent (or lack thereof) for processing.

Each case shall be managed on an individual basis.

This policy shall not apply to CCTV systems or other measures employed to insure the safety and security of participants, except that individuals will always be informed of the presence of such systems.

ECO-UNESCO do not employ any systems capable of carrying out facial recognition.

Employee Training

ECO-UNESCO appreciates that as we continue to invest in ensuring our systems are structured and configured to protect the data which we hold, it is vital that we continue to invest in employee training and awareness.

ECO-UNESCO commit to ensuring:

- All new employees shall receive training on Data Protection.
- All employees shall receive refresher training on Data Protection and Data Security once per year.
- All employees, upon leaving the organisation, shall be requested to confirm that they have returned or destroyed all data in their possession belonging to ECO-UNESCO.

Glossary of terms

| | |
|--------------------------------|---|
| | |
| Data 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law |
| Data Processor | ... means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller |
| Processing | ... any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction |
| Personal Data | ... any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; |
| Sensitive Personal Data | ... personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited |

Review

This policy will be reviewed annually, or to address changes in the law.

Version History

| Date | Version | Description |
|------------------------|-------------|--|
| 1 May 2018 | 2018.05 | Policy re-written to reflect requirements under GDPR |
| 13 October 2014 | Version 1.0 | Policy Adopted by the Board of ECO-UNESCO |