

Ireland's Content Pool, Privacy Policy

1. WHO WE ARE

This privacy policy (the "Policy") refers to the digital asset management system called Ireland's Content Pool (DAM), the website; www.irelandscontentpool.com (the "System").

Ireland's Content Pool is operated jointly by Tourism Ireland Limited whose principal place of business is at 5th Floor Bishop's Square, Redmond's Hill, Dublin, D02 TD99, Ireland and Fáilte Ireland whose principal place of business is at 88-95 Amiens Street, Dublin, DO1 WR86 ("we", "our", "Tourism Ireland", "Fáilte Ireland").

Your privacy is of paramount importance to us. This Policy is designed to protect you, our users, by informing you what Personal Data is collected, how we will use the information about you, with whom we share it, how long we keep it and how to contact us if you have any queries or concerns about our use of your personal information. Your use of the System is subject to your agreement with this Policy.

In this Policy, the term "**Personal Data**" means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, our possession, and includes Personal Data as described in Data Protection Laws (as defined below). Any Personal Data that we collect from you for the purposes described in this Policy is hereinafter referred to together as "**Your Data**".

Please read the following carefully. Registering for an account ("**Your Account**") or entering into this System and providing your consent to our use of Your Data in accordance with the terms of this Policy indicates that the user has reviewed this Policy and has agreed to be bound by it. If you do not agree to these terms you must leave the System immediately. We will keep a record of your consent in this regard. If you no longer consent to our processing of Your Data, you may request that we cease such processing by contacting us via the 'How to Contact Us' facility referred to below.

We will handle Your Data in accordance with Data Protection Laws. "**Data Protection Laws**" means the Data Protection Acts 1988 to 2018, the General Data Protection Regulation (EU) 2016/679 ("**GDPR**"), and any other applicable law or regulation relating to the processing of Personal Data and to privacy, including the E-Privacy Directive 2002/58/EC and the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011, as such legislation shall be supplemented, amended, revised or replaced from time to time and all guidance and codes of practice issued by a relevant supervisory authority from time to time and which are applicable to us.

We are a controller (as defined in Data Protection Laws) in relation to any Personal Data which we collect from you through your or any other user's use of the System and the set-up of Your Account. This Policy sets out the basis on which any such Personal Data will be processed by us. You may be a data subject (as defined in Data Protection Laws) or you may be a controller. When you are a controller in respect of the Personal Data of other data subjects, then you must comply with all of your controller obligations under Data Protection Laws. When you are a controller, we and you act as independent controllers, unless agreed otherwise.

2. WHAT IS THE CONTENT POOL USED FOR?

The Content Pool is an online repository of free promotional images, videos, branding and other marketing assets available for you to positively promote tourism on the Island of Ireland. This is a tri-agency collaboration between Fáilte Ireland, Tourism Ireland and Tourism Northern Ireland, inspiring all registered users to avail of a wide range of top-quality digital marketing assets.

3. INFORMATION WE GATHER FROM YOU

We fully respect your right to privacy in relation to your interactions with the System and endeavour to be transparent in our dealings with you as to what information we collect and how we use your information. We only collect and use individual's information where we are legally entitled to do so. Information in relation to Personal Data collected by Irish entities is available on www.dataprotection.ie, the website of the Irish Data Protection Commission ("DPC").

For the purpose of registering for the System, the information collected will include your name and email address.

Portal usage information is collected using cookies. We collect and collate generic information on all our System traffic that is only ever represented in aggregate format. For more information, please see our [Cookies Policy](#).

From time to time, we may ask users for feedback (free text entry, quality ratings or similar) to help analyse the quality and performance of the System. Information collected for this purpose is done so anonymously where you agree to participate and is used to aid our understanding of customer needs and opinions only. On occasion specific quotes may be highlighted from individuals, however this is done so without personally identifying the users.

Applications developed in connection with the System for mobile devices will operate and capture information as set out above and are also subject to this Policy.

We endeavour to keep Your Data accurate and up-to-date. As such, you must tell us about any changes to such information that you are aware of as soon as possible

Our System is not intended for children and we do not knowingly collect personal data relating to children. If you are aged under 18, please get your parent/guardian's permission before you provide Your Data to us/use the System.

If we receive notice or believe that we have been provided with Personal Data on anyone under 18, we will make reasonable efforts to remove such Personal Data from our records. We reserve the right to seek verification of your age where we deem it appropriate to do so.

4. WHY WE COLLECT/HAVE ACCESS TO YOUR INFORMATION

We may collect information from you as necessary in the course of providing our service. We may collect your personal information while monitoring our technology tools and services, including our System and email communications sent to and from us. We gather information about you when you provide it to us or interact with us directly.

We collect information about you to help us to manage Your Account.

We collect IP addresses from visitors to our System (an IP address is a number that can uniquely identify a specific computer or other network device on the internet). This allows us to identify the location of users, to block disruptive use and to establish the number of visits from different countries. We analyse this data for trend and statistics reasons, such as which parts of our System users are visiting and how

long they spend there.

We may use Your Data on any one or more of the following legal bases: (i) to perform a contract with you; (ii) for our legitimate business purposes in providing the service to you (in which case, our legitimate interests will not override your fundamental privacy rights); and/or (iii) where you have given us your express consent (e.g. for direct marketing purposes, as set out above).

We have set out below, in a table format, a description of all the ways we plan to use Your Data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are, where appropriate.

Note that we may process Your Data for more than one legal basis depending on the specific purpose for which we are using your data. Please contact us if you need details about the specific legal basis we are relying on to process Your Data where more than one ground has been set out in the table below.

Purpose	Categories of Data	Legal basis for processing and, where necessary, the basis of legitimate interest
To respond to an enquiry from you.	basic information, and contact information.	Necessary to respond to a query from you to provide you with information to fulfil mutual legitimate interests.
To register you as a customer of our System.	basic information, contact information, profile information	To provide you with a service where you can register to access tourism digital assets that interest you.
To make suggestions and recommendations to you about services that may be of interest to you.	Basic information, contact information, profile information	To provide you with a service where you can be notified of upcoming events that may be of interest to you, to fulfil mutual legitimate interests.
To administer and protect our business and the System (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data).	Basic information, contact information, profile information, and technical information	Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation or group restructuring exercise).

Purpose	Categories of Data	Legal basis for processing and, where necessary, the basis of legitimate interest
To provide and improve our System, including auditing and monitoring its use, providing and improving our service to you and managing and administering our relationship with you.	basic information, contact information, technical information, including IP address	Necessary for our legitimate interests to provide and improve our System, including auditing and monitoring its use; providing and improving our service to you; or managing and administering our relationship with you; IP to direct you to the local version of our website. Necessary to fulfil our legal, regulatory and risk management obligations.

5. USER UPLOADED DATA

Your Data is separate from and should be distinguished from User Uploaded Data. “User Uploaded Data” is data uploaded by you or others through Your Account/your use of the System when you use e.g. the comment function, contact us function or ‘Upload Assets’ function on our System. We strongly recommend that you avoid uploading any Personal Data in any User Uploaded Data. We reserve the sole right to review, edit or delete User Uploaded Data. We also moderate all User Uploaded Data in order to ensure that it does not contain Personal Data. Notwithstanding this, we are a Processor and you are the Controller in respect of User Uploaded Data (to the extent that it includes Personal Data).

If you are a Controller in respect of any Personal Data of other data subjects contained in User Uploaded Data, then you must comply with all of your Controller obligations under Data Protection Laws in that regard.

If you upload assets you must verify that you have full documented copyright, marketing usage rights and consent of all related parties to use and to share any assets containing people for the purposes of promoting their business.

6. MODEL RELEASE AND LOCATION RELEASE DOCUMENTS

When commissioning visual content we will request model releases from those subjects featuring in images and video as well as location releases from the owners or stewards of the properties where photography or imagery has taken place.

We retain model and location release documentation in digital format within Ireland’s Content Pool and in hard copy format on file within a secure location. Access to these release documents is strictly controlled. The release documents are retained to ensure that the rights of use of the visual assets are managed appropriately.

7. WHAT RIGHTS DO YOU HAVE

As a data subject, you have the following rights under Data Protection Laws and we, as controller in respect of Your Data, will comply with such rights in respect of Your Data. These rights are explained in more detail below, but if you have any comments, concerns or complaints about our use of Your Data, please contact us (see 'How to Contact Us' below). We will respond to any rights that you exercise within one month of receiving your request, unless the request is particularly complex, in which case we will respond within three months (we will inform you within the first month if it will take longer than one month for us to respond).

Right	Further Information
Right of Access (Article 15 GDPR)	You have the right to request a copy of Your Data. Requests for Your Data must be made to us (see 'How to Contact Us' below) specifying what Personal Data you need access to, and a copy of such request may be kept by us for our legitimate purposes in managing the System. To help us find the information easily, please give us as much information as possible about the type of information you would like to see. If, to comply with your request, we would have to disclose information relating to or identifying another person, we may need to obtain the consent of that person, if possible. If we cannot obtain consent, we may need to withhold that information or edit the data to remove the identity of that person, if possible. We are also entitled to refuse a data access request from you where (i) such request is manifestly unfounded or excessive, in particular because of its repetitive character (in this case, if we decide to provide you with the Personal Data requested, we may charge you a reasonable fee to account for administrative costs of doing so); or (ii) we are entitled to do so pursuant to Data Protection Laws. For security reasons, we will take reasonable steps to confirm your identity before providing you with any Personal Data we may hold about you.
Right of Rectification (Article 16 GDPR)	You have the right to request that we amend any inaccurate or incomplete Personal Data that we have about you. If you would like to do this, please (i) email or write to us (see 'How to Contact Us' below); (ii) let us have enough information to identify you (e.g. name, registration details); and (iii) let us know the information that is incorrect and what it should be replaced with. If we are required to update Your Data, we will inform recipients to whom that Personal Data have been disclosed (if any), unless this proves impossible or has a disproportionate effort. It is your responsibility that all of the Personal Data provided to us is accurate and complete. If any information you have given to us changes, please let us know as soon as possible (see 'How to Contact Us' below).

Right to Object (Article 21 GDPR)	You have the right to ask us to stop using Your Data, and we will comply unless there is a legal basis for us to continue using it, which we will explain to you.
Right to Erasure (Article 17 GDPR)	You can ask us to erase Your Data (i) where we do not need Your Data in order to process it for the purposes set out in this Policy; (ii) if you had given us consent to process Your Data, you withdraw that consent and we cannot otherwise legally process Your Data; (iii) you object to our processing and we do not have any legal basis for continuing to process Your Data; (iv) Your Data has been processed unlawfully or have not been erased when it should have been; or (v) the Personal Data have to be erased to comply with law. We may continue to process Your Data in certain circumstances in accordance with Data Protection Laws. Where you have requested the erasure of Your Data, we will inform recipients to whom that Personal Data has been disclosed, unless this proves impossible or involves disproportionate effort. We will also inform you about those recipients if you request it.
Right to Restriction of Processing (Article 18 GDPR)	You may request that we stop processing Your Data temporarily if (i) you do not think that Your Data is accurate (but we may start processing again once we have checked and confirmed that it is accurate); (ii) the processing is unlawful but you do not want us to erase Your Data; (iii) we no longer need the Personal Data for our processing; or (iv) you have objected to processing because you believe that your interests should override the basis upon which we process Your Data. If you exercise your right to restrict us from processing Your Data, we will continue to process the Personal Data if: (i) you consent to such processing; (ii) the processing is necessary for the exercise or defence of legal claims; (iii) the processing is necessary for the protection of the rights of other individuals or legal persons; or (iv) the processing is necessary for public interest reasons.
Right to Data Portability (Article 20 GDPR)	You may ask for an electronic copy of Your Data that you have provided to us and which we hold electronically, or for us to provide this directly to another party. This right only applies to Personal Data that you have provided to us – it does not extend to data generated by us. In addition, the right to data portability also only applies where (i) the processing is based on your consent or for the performance of a contract; and (ii) the processing is carried out by automated means.
Right to be Informed	You have the right to clear, transparent and easily understandable information about your rights and about how we use Your Data. We use this Policy to inform you of your rights.
Right to Withdraw Consent	Where processing is based on your consent, you have the right to withdraw your consent at any time with future effect by contacting us. However, if you do withdraw your consent we may not be able to continue to provide the service we offer to you.

Right to ask us to stop contacting you with direct marketing	We have a legitimate interest to send you electronic communications in connection with the System and related matters (which may include but shall not be limited to newsletters, announcement of new features etc. and which may also appear on social media platforms such as Facebook, LinkedIn, X or Instagram). We may also ask you for your consent to send you direct marketing from time to time. You may be able to select your preferences with respect to direct marketing when registering Your Account. We may also ask you different questions for different services, including competitions. We may also ask you to complete surveys that we use for research purposes, although you do not have to respond to them. You have the right to ask us to stop using Your Data: • at any time where it is being used for direct marketing (including profiling); or • if we process Your Data (including profiling) because it forms part of our public tasks or is in our legitimate interests. We will comply with your objection unless there are compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. We may continue to process Your Data for other purposes that do not relate to performing our public tasks or pursuing our legitimate interests. If you would like to exercise your right to object to processing Your Data for direct marketing or any other purposes, you can do so by contacting us (see 'Error! Reference source not found.. How to Contact Us' below) (this can take up to 5 working days).] We will provide you with information on action taken on a request to stop direct marketing - this may be in the form of a response email confirming that you have 'unsubscribed'. Unsubscribing from direct marketing does not unsubscribe you from essential electronic communications in respect of the administration of Your Account.
Rights in relation to automated decision making	We do not attempt to collect further data without user consent that enables personally identifiable profiling of our users.
Right to Complain to the DPC	If you do not think that we have processed Your Data in accordance with this Policy, please contact us in the first instance (see 'How to Contact Us' below). If you are not satisfied, you can complain to the DPC or exercise any of your other rights pursuant to Data Protection Laws. Information about how to do this is available on the DPC website at https://www.dataprotection.ie.

8. WHO WE SHARE YOUR INFORMATION WITH

We will share Your Data with various third parties (subject to having appropriate contracts in place) including:

Fáilte Ireland [Failte Ireland](#) and Tourism Northern Ireland [Tourism NI](#) our sister agencies and joint partners of the System.

[Orange Logic | Scalable Digital Asset Management \(DAM\) Software](#) who assist us in the provision of the System.

We may disclose your personal information to any business unit, company or other corporate entity under the control and direction of Tourism Ireland. We do not sell or pass on your personal details to third parties without your consent, except in the following, highly unlikely, instances:

- ♣ where it is required by applicable law or pursuant to a court or similar order
- ♣ where it is required urgently to prevent serious loss or damage to property of Tourism Ireland or Fáilte Ireland
- ♣ where it is required for the purposes of obtaining legal advice or for the purposes of, or in the course of, legal proceedings to which Tourism Ireland or Fáilte Ireland is a party or a witness.

9. WHAT INTERNATIONAL TRANSFERS WITH YOUR DATA DO WE MAKE?

It is sometimes necessary for us to transfer (including transmission, storage and remote access) Your Data to countries outside the European Economic Area (“EEA”) or the UK. The EEA, UK and other countries outside the EEA have data protection laws that differ from the Data Protection Law, some of which may provide lower levels of protection of Personal Data or privacy rights.

As we are based in Ireland and the United Kingdom, we will transfer Your Data to:

- our affiliates located in Ireland, other countries in the EEA, the United Kingdom and other countries outside the EEA.
- our contractors and service providers located in Ireland, other countries in the EEA, the United Kingdom or other countries outside the EEA. For example:
 - if you consent to our use of targeting cookies, Your Data (a unique identifier associated to you) will be sent to the United States. For more information on these recipients, see our Cookies Policy.
 - the jurisdiction from where you access our System.

Unless otherwise permitted by Data Protection Laws, we will only transfer Your Data to a territory outside the EEA where an adequate or equivalent degree of data protection is assured. We will take all steps reasonably necessary to ensure that Your Data is treated securely. Such safeguards in place with regard to the transfer of Your Data to third countries include

in the case of transfers subject to the GDPR:

- (a) the country is subject to an ‘adequacy decision’ which means it has been deemed to provide an adequate level of protection for Personal Data by the European Commission under Article 45 of the GDPR. A list of countries the European Commission has currently made adequacy decisions in relation to is [available here](#). For example, we rely on adequacy decisions for transfers to the United Kingdom and the United States;
- (b) we enter into appropriate contracts with third parties incorporating standard contractual clauses approved by the European Commission under Article 46(2) of the GDPR together

with any supplementary measures required appropriate to any risks in the transfer. For further details, see [European Commission: Standard contractual clauses for data transfers between EU and non-EU countries](#). For example, we rely on standard contractual clauses for transfers to the following countries: United States.;

- (c) there are other appropriate safeguards that comply with Chapter V of the GDPR in place, together with enforceable rights and effective legal remedies for you; or
- (d) a specific exemption applies that is permitted by Article 49 of the GDPR.

In the case of transfers subject to the UK GDPR:

- (a) the country is subject to an adequacy regulation which means it has been determined by the government of the United Kingdom to provide an adequate level of data protection under Article 45 of the UK GDPR. A list of countries the United Kingdom currently has adequacy regulations in relation to is [available here](#). We rely on adequacy regulations for transfers from the United Kingdom to Ireland and other EEA member states;
- (b) there are other appropriate safeguards that comply with Article 46 of the UK GDPR in place, together with enforceable rights and effective legal remedies for you; or
- (c) a specific exemption applies that is permitted by Article 49 of the UK GDPR.

All information you provide to us is stored on our (or contracted third party) secure servers. Where we have given you (or where you have chosen) a password which enables you to access any part of our System, you are responsible for keeping this password confidential. We ask you not to share your password with any person not authorised to use the System.

For more information on transfers of Your Data, please contact us (see 'How to Contact Us' below).

10. THIRD PARTY WEBSITES

This Policy applies to the System operated by us. We do not exercise control over the sites/applications that may be linked from the System. These other sites/applications may place their own cookies or other files on your computer, collect data or solicit personal information from you. You acknowledge that the service that we provide may enable or assist you to access the System content of, correspond with, and purchase goods and services from, third parties via third-party websites and that you do so solely at your own risk. We make no representation or commitment and shall have no liability or obligation whatsoever in relation to the content or use of, or correspondence with, any such third-party website, or any transactions completed, and any contract entered into by you, with any such third party and the use by any such third-party of Your Data. We do not endorse or approve any third-party website nor the content of any of the third-party website made available via the System. We encourage you to carefully familiarize yourself with the terms of use and privacy policies applicable to any websites and/or services operated by third parties. Please be aware that we are not responsible for the privacy practices of any third parties.

11. OFFENSIVE CONTENT

If Your Data contains any material which may reasonably be deemed to be offensive, inappropriate or objectionable or otherwise engage in any disruptive behaviour in relation to the System, we may remove such content and/or suspend the use of Your Account.

Where we reasonably believe that you are or may be in breach of any applicable laws, for example on hate speech, we may disclose your personal information to relevant third parties, including to law

enforcement agencies or your internet provider. We would only do so in circumstances where such disclosure is permitted under applicable laws, including Data Protection Laws.

12. HOW DO WE PROTECT YOUR PERSONAL INFORMATION

We do our utmost to protect user privacy through the appropriate use of security technology. We restrict access to Your Data to employees, contractors and agents who need to know Your Data in order to operate, develop or improve the services that we provide. We ensure that we have appropriate physical and technological security measures to protect your information; and we ensure that when we outsource any processes that the service provider has appropriate security measures in place. However, our System may contain hyperlinks to websites owned and operated by third parties. These third party websites have their own privacy policies, including cookies. We do not accept any responsibility or liability for the privacy practices of such third party websites and your use of such websites is at your own risk.

We will implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks that are presented by the processing of Your Data. In particular, we will consider the risks presented by accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Your Data transmitted, stored or otherwise processed.

Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect Your Data, we cannot guarantee the security of any data transmitted to us and any such transmission is at your own risk. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access. To the extent permitted by law, we are not responsible for any delays, delivery failures, or any other loss or damage resulting from (i) the transfer of data over communications networks and facilities, including the internet, or (ii) any delay or delivery failure on the part of any other service provider not contracted by us, and you acknowledge that our service may be subject to limitations, delays and other problems inherent in the use of such communications facilities. You will appreciate that we cannot guarantee the absolute prevention of cyber-attacks such as hacking, spyware and viruses. Accordingly, you will not hold us liable for any unauthorised disclosure, loss or destruction of Your Data arising from such risks.

13. BREACH REPORTING

We will notify serious data breaches in respect of Your Data to the DPC without undue delay, and where feasible, not later than 72 hours after having become aware of same. If notification is not made after 72 hours, we will record a reasoned justification for the delay; however, it is not necessary to notify the DPC where the Personal Data breach is unlikely to result in a risk to the rights and freedoms of natural persons. A Personal Data breach in this context means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

We will keep a record of any Personal Data breaches, including their effects and the remedial action taken, and will notify you of any Personal Data breach affecting Your Data (which poses a high risk to you) when we are required to do so under Data Protection Laws. We will not be required to notify you of a Personal Data breach where:

- we have implemented appropriate technical and organisational measures that render the Personal Data unintelligible to anyone not authorised to access it, such as encryption; or
- we have taken subsequent measures which ensure that the high risk to data subjects is not likely to materialise; or

- it would involve disproportionate effort, in which case we may make a public communication instead.

14. RETENTION OF PERSONAL DATA

Your Data will be kept and stored for such period of time as we deem necessary taking into account the purpose for which it was collected in the first instance. This may include retaining Your Data as necessary to administer Your Account, comply with our legal obligations, to resolve disputes, to enforce our agreements, to support business operations, and to continue to develop and improve our service.

We generally keep Your Data for 3 years after you stop engaging with us, e.g. accessing the Portal. We then delete Your Data from our databases.

For further information on the period for which we retain Your Data or the criteria we use to determine that retention period, please contact us (see '15. How to contact us?' below).

For more information on how long cookies and other identifiers are stored, please see our Cookies Policy.

Where we retain information for service improvement and development, we take steps to eliminate information that directly identifies you, and we only use the information to uncover collective insights about the use of our System, not to specifically analyse personal characteristics about you.

15. CHANGES TO THIS POLICY

We may change this Policy from time to time and at our sole discretion. The date of the most recent revisions will appear on the top of this Policy. If you do not agree to these changes, please do not continue to use the System to submit Your Data. If material changes are made to this Policy, we will notify you by placing a prominent notice on our System or by sending you a notification in relation to this. We will not process Your Data in a manner not contemplated by this Policy without your consent.

16. HOW TO CONTACT US

If you need to contact us with regard to any of your rights as set out in this Policy, all such requests should be made in writing by email to dpo@tourismireland.com.

You can contact us and our Data Protection Officer by post, email or telephone, if you have any questions about this Policy or Your Data, to exercise a right under Data Protection Law (see further under '7. What data protection rights do you have?' above), or to make a complaint.

Agency	Address	Telephone number	Data Protection officer contact details
Tourism Ireland	5th Floor Bishop's Square, Redmond's Hill, Dublin D02 TD99, Ireland	+353 1 476 3400	dpo@tourismireland.com

Fáilte Ireland	85-95 Amiens Street, Dublin 1 Dublin, D01 WR86, Ireland	+353 (0)1-5741990	dataprotection@failteireland.ie
Tourism Northern Ireland	10-12, Linum Chambers, Bedford St, Belfast BT2 7ES	+44 28 90441536	See Tourism Northern Ireland's Privacy Policy for DPO contact details

Latest Update Sept 2025