



An Chomhairle Oidhreachta
The Heritage Council

Data Protection Policy

Version	V 2
Owner	The Heritage Council
Date	June 2024
Approved	

Table of Contents

1. Who we are.....	1
2. How to contact us.....	1
3. Corporate GDPR Statement.....	1
4. What is GDPR?.....	2
5. What is data?.....	2
6. What is personal data?.....	3
7. Principles of data protection.....	3
8. What personal data we handle & what we do with it.....	4
9. What we will not do with your personal data.....	6
10. How long we keep your personal data for.....	6
11. When do we transfer data to third countries.....	6
12. Who do we share your personal data with.....	7
13. Your rights as a Data Subject.....	7
14. Making a Data Access request.....	8
15. Other Data Subject rights.....	9
16. Making a complaint.....	9
17. Responsibilities of Staff, Contractors & Council Members.....	10
18. Project Planning and GDPR.....	10
19. Photographs and videos featuring people.....	10
20. Keeping data secure.....	12
21. Changes to this policy.....	13
 Appendix A Data Retention Schedule and Policy.....	 14
Appendix B Template Consent Form for Filming and Photography.....	27
Appendix C Template Filming/Photography Location Warning Notice.....	29

1 Who we are

Established under The Heritage Act 1995, the Heritage Council is a public body whose mission is to develop a wide understanding of the vital contribution that our heritage makes to our social, environmental & economic well-being.

The Heritage Council provides policy advice for government on heritage issues that include sustainability, landscape management, built and cultural heritage, forestry and climate change.

The Heritage Council encourages and promotes interest in heritage through our education programmes.

Through our publications, social media, promotions and through National Heritage Week, the Heritage Council raises awareness and engages with the public about heritage.

We work with local communities through our Heritage Officer programme. We provide support to local communities to carry out heritage related activities and projects through our Community Heritage Grant Scheme.

The Heritage Council works with partners, particularly at local level, to increase awareness of our national heritage and to highlight its importance to public policy and everyday life.

We support the heritage sector through our programmes and initiatives.

2 How to contact us

The Heritage Council is located at Áras na hOidhreachta, Church Lane, Kilkenny, R95 X264.

Our Data Protection Officer can be contacted

- By telephone at 056 7770777
- By email at dpo@heritagecouncil.ie
- By post at Data Protection Officer, The Heritage Council, Áras na hOidhreachta, Church Lane, Kilkenny, R95 X264.

3 Corporate GDPR Statement

In order to provide effective service to stakeholders, grant recipients, council members and employees, The Heritage Council will be required to collect, process and use certain types of personal data. The Heritage Council will, through its actions and policies, demonstrate that it cares for the personal data of people it interacts transparently, accountably, securely and in their interest in the first instance, and in the public interest thereafter, and that it will manage and monitor on an on-going basis its responsibilities as a 'data controller' in relation to the GDPR.

The Heritage Council undertakes to process all personal data with care for its ownership and integrity, and in accordance with the principles of GDPR. It will ensure that appropriate security measures are in place to protect confidentiality and will review these from time to time with due regard to the technology available, the cost and the risk of unauthorised access.

This Policy supports the provision of a management structure to assist the Heritage Council to comply with its obligations under GDPR, including the application of best practice guidelines and procedures in relation to all aspects of data protection. It shall be reviewed and updated in accordance with any legislative changes or other relevant indicators.

This Policy is to be read in conjunction with The Heritage Council Staff Handbook, Information Technology Security Policy, Anti-Fraud Policy, Data Privacy Policy, Subject Access Request Policy. These associated documents contain important corroborative guidance as to how Council discharges its Data Protection duties.

4 What is GDPR?

The General Data Protection Regulation (GDPR) replaces and deepens the data protection laws that existed in the European Union pre-25th May 2018.

Its purpose is to safeguard the privacy rights of individuals in relation to the 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 of their personal data.

Data protection relates to you in two important ways:

- As a data controller the Heritage Council holds, uses and processes personal data (about living persons) as part of its job.
- As a data subject where Council as an employer holds, uses and processes the personal data of its members staff and associates.

5 What is data?

Data and information may be held in the following formats:

- Paper records
- Application forms
- Text messages
- Whatsapp messages
- Electronic files on shared drives
- Electronic files on own computer files
- Emails
- Diaries
- Accounts

- Registers
- Notebooks
- Tapes, DVDs, CDs
- Servers
- Websites
- Drawings, maps
- Photographs, images

Data can be stored on cloud services, computer networks, hard drives, USB sticks, internet, phone systems, mobile devices (smartphone or tablet), cameras, SD cards, hard copy paper files, electronic files, CCTV systems, voice recordings, etc.

6 What is Personal Data?

Personal data means information 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, your possession.

Examples of personal data include name, address, phone number, email address, date of birth, bank details, signature, PPSN, photograph, video footage, employment records, salary records, medical records, a computer's IP address, voicemail, biometric data, etc. This list is not exhaustive.

Data Protection relates exclusively to personal data held on a living individual who is, or can be, identified from that data.

The key to GDPR compliance involves ensuring that personal data held on individuals is:

- Gathered only in relation to its statutory purposes, or with the consent of the data subject
- Published or disclosed only when consent is obtained
- Kept up-to-date and accurate
- Retained only for as long as is absolutely necessary
- If stored in Council's archives, then only for purposes related to heritage objects, and only for the purposes of identifying those objects
- Not used for any purpose other than that consented to by the individual.

7 Principles of Data Protection

As a data controller, there are 8 rules that must be followed. The Heritage Council, its staff and members must:

- Obtain and process information fairly. At the time when information is collected on individuals, they must be made aware of how that information is going to be used. If it is intended to use this data for secondary purposes, the data subject must be informed of these purposes and explicitly consent to this use of their personal data.

- Keep it for a specified, explicit and lawful purpose. The purpose for which personal information on living individuals is retained must be made clear. It must be a lawful purpose e.g. legally or contractually necessary or necessary for the performance of a public body's function.
- Use and disclose it only in ways compatible with this purpose. Any use or disclosure must be necessary for and compatible with the purpose for which the data was collected and kept.
- Keep it safe and secure. Adequate security provisions must be in place to protect personal data.
- Keep it accurate, complete and up to date. Data must be checked to ensure it is accurate and contemporaneous i.e. it must be updated over time.
- Ensure that it is adequate, relevant and not excessive. Where personal data is collected, we must be able to justify every piece of information held on a given individual.
- Retain it for no longer than is necessary. Personal data must only be kept for as long as it is needed for the purpose for which it was collected.
- Make it accessible to that individual, and only that individual, on request. Individuals should be informed of their right to get a copy of all personal data held on them.

8 What personal data we handle and what we do with it

Detailed information data processing for each of our programmes and grant schemes is available in our retention schedule in Appendix A.

In order to comply with the GDPR Regulations and to ensure that the highest possible standards of protection are given to personal data, the Heritage Council will maintain a Records of Processing Activity (RoPA). A RoPA outlines each of the processing activities undertaken by the Heritage Council, the legal basis for doing so, the location of the data and how long it will be processed for. Further information on our RoPA can be found in our Records of Processing Activity procedure.

For the purpose of fulfilling the Heritage Council's functions, we perform the following processing activities:

(a) Processing grant scheme applications

The Heritage Council processes personal data through our online grant scheme system. The lawful basis for processing this data is to provide grant applicants with funding.

(b) Interact with the general public

From time to time the members of the public contact the Heritage Council for advice, to request a copy of a publication or to enquire about the work of the Heritage Council. In doing so, they provide us with contact details. The lawful basis for processing this data is consent. Members of the public interact with us through email, written letter, telephone and social media. The Heritage Council IT Policy outlines the standards of security surrounding data received via electronic means and mobile devices.

(c) Process CCTV footage

At our headquarters, in Áras na hOidhreachta, CCTV is in operation for the purposes of security and safety of our staff and visitors. Lawful basis for processing is the legitimate interests of the Heritage Council.

(d) Process recruitment applications

We process personal information provided to us from prospective candidates during recruitment campaigns. This personal data is processed in necessity for the compliance with the legal obligations of the data controller.

(e) Perform a contract

When paying suppliers, grant recipients and contractors we will process personal data. This is done in accordance with performing a contract to which the data subject is party.

(f) Provide information through our websites

The Heritage Council processes personal data such as strictly necessary cookies for any user of our websites, www.heritagecouncil.ie; www.heritageweek.ie; www.heritageinschools.ie; www.iwtn.ie; www.heritagemaps.ie

Cookie policies, which form part of our Data Protection Policy, can be found here:

<https://www.heritagecouncil.ie/site-info/cookie-privacy>

<https://www.heritageweek.ie/site-info/cookie-privacy-policy>

<https://www.heritageinschools.ie/about/cookie-privacy-policy>

<https://irishwalledtownsnetwork.ie/cookie-policy-eu/>

(g) Comply with legal requirements

As a public body, the Heritage Council is required to cooperate with internal and external audits. As part of this process, we may need to share personal information such as the information contained on invoices or recruitment data.

(h) Organise events

From time to time the Heritage Council will organise events which are open to the public to attend. These may include Heritage Week training and awards events and public events at our offices in Kilkenny. Personal data may be collected in order to communicate with those interested in attending our events.

(i) Automated decision making

The Heritage Council uses automated decision making as part of the grants process. Applicants are required to answer a number of yes/no eligibility questions before they can apply for a Grant. If the applicant does not respond to the questions to indicate their eligibility, they cannot proceed to the next step of the application. Applicants can contact a member of the Grants Team if they believe that they are eligible to apply for the scheme.

9 What we will not do with your personal data

(a) Direct Marketing

The Heritage Council does not engage in direct marketing.

(b) Record telephone communications

The Heritage Council does not audio record or retain audio recordings of phone conversations. We may only record personal data in the form of notes taken during a telephone conversation in order to further reply to and assist the individual with their query.

10 How long do we keep your personal data

The length of time that the Heritage Council holds personal data for depends on the processing operation carried out with the data.

The processing of data associated with using our websites, www.heritagecouncil.ie; www.heritageweek.ie; www.heritageinschools.ie; www.iwtn.ie; www.heritagemaps.ie, or cookies, is outlined in the cookie policy of the respective websites.

The processing of data associated with other activities is outlined in the retention schedule in Appendix A.

11 When do we transfer your personal data to third countries

Transfer of personal data to third countries is prohibited unless safeguards are in place to protect the rights and freedoms of data subjects. This also includes information saved in the cloud.

The Data Protection Officer must be consulted prior to any project that may involve transfer of data outside of the EU.

12 Who we share your personal data with

The Heritage Council will not share personal data unless there is a legal basis for doing so.

Data may be shared with:

- (a) To a third party for the joint processing of personal data (e.g. IT provider, Department of Agriculture)
- (b) To fulfil a legal obligation (e.g. revenue for the processing of payroll)
- (c) To a third party for the purpose of providing a service (e.g. courier)

Data sharing will be documented in our retention schedule and Record of Processing Activity (RoPA).

Where personal data, collected by the Heritage Council, is hosted, processed or held by third party service providers, GDPR compliance requirements must be included in all contracts with the party hosting, processing or holding the data.

All contracts must explicitly state:

- The nature, purpose and duration of hosting, processing or holding personal data.
- The type of personal data and categories of data subjects.
- Personal data cannot be used, reused, disclosed, or shared with another party for any purpose(s) other than those specifically agreed upon and referred to in the contract.
- Personal data must be stored securely in accordance with European best practice operating and certification standards, and not US equivalents, in accordance with Article 32 of the GDPR. The location of the data must be clearly identified.
- Personal data must be retained only as long as is absolutely necessary to perform the specified contractual service. It is the responsibility of the service provider to ensure that data (including copies) is permanently and securely deleted once it is no longer needed.
- Third parties who engage in marketing/ mailing services on behalf of the Heritage Council must ensure that all recipients (current and new) have 'actively' consented to receiving these communications. Where de-registration is requested, the data subject's details must be removed immediately from mailing lists and the data subject must be informed that this has actually occurred. Every communication must include a consent 'opt out' facility.

13 Your Rights as a Data Subject

As a data subject, you have the following rights:

- Right to have your personal data used in accordance with GDPR. Your personal information must be obtained and used fairly, kept securely and only for as long as is absolutely necessary, and not illegitimately disclosed to others.
- Right to be informed about the type and extent of personal data collected or obtained from you and held by commercial companies and other organisations.

- Right of access to your personal data. You are entitled to get a copy of your personal information.
- Right to rectification. You have the right to have your personal information corrected where it is inaccurate or completed where it is incomplete.
- Right to be forgotten. You have the right to have your personal data erased if it is being un-lawfully processed, held for longer than necessary, or used for direct marketing purposes.
- Right to data portability allows data subjects to get back personal data they provided to an organisation in a structured, commonly used and machine-readable format.
- Right to object to processing of your personal data, particularly where it relates to direct marketing or profiling.
- Right to restrict processing of your personal data. Where processing of your data is restricted, it can be stored by the data controller, but most other processing actions - for example deletion - will require your permission. A typical example is where you have contested the accuracy of your data and request a restriction until the data controller has determined the accuracy of your data, or the outcome of your objection.
- Right to freedom from automated decision-making. You have the right not to be subject to a decision based solely on automated processing.

14 Making a Data Access Request

Data subjects are entitled to request copies of any personal details held on them by the Heritage Council, free of charge. The Heritage Council will provide this information within one month from date of receipt of the request, or sooner if possible. The Heritage Council will use reasonable means to verify the requester's identity as the relevant data subject.

Data subjects must submit a request in writing stating the exact information required.

Requests by email should be sent to: dpo@heritagecouncil.ie

Requests by post should be sent to: The Data Protection Officer, The Heritage Council, Church Lane, Kilkenny, R95 X264.

The data subject is only entitled to information that relates to them and will not be provided with data relating to other people or third parties.

Employees who record opinions about other employees in the course of their employment should bear in mind that these opinions may be disclosed to the data subject under an access request.

Please Note: The Heritage Council promotes an open access policy when dealing with data requests. Where possible, data requests shall be dealt with informally, outside of formal GDPR procedures.

Further information on subject access requests can be found in our Subject Access Request Policy.

15. Other Data Subject Requests

Data subjects may request to invoke rights, other than access requests under GDPR. They may make a request to be forgotten, e.g. for their data to be erased. They may request for their data to be rectified if the data held on them is incorrect. They may object to their data being processed or wish for their data to be limited in processing.

Where a data subject requests for the Heritage Council to cease processing their data or for their data to be erased, their request will be responded to within one month, subject to the lawfulness of processing.

Incorrect information will be updated upon request.

Any requests from data subjects in relation to their rights should be forwarded to the Data Protection Officer.

16. Making a Complaint

Under Article 77 of the GDPR, a data subject has the right to lodge a complaint with the Data Protection Commission if you consider that your personal data is being processed contrary to your rights under GDPR.

Under Article 78 of the GDPR, a data subject has the right to an effective judicial remedy where the Data Protection Commission does not handle your complaint or does not inform you, within three months, on the progress or outcome of your complaint.

Under Article 80, a data subject may authorise certain third parties to make a complaint on their behalf.

Complaints to the Commission should be submitted in writing and addressed to:

info@dataprotection.ie

or

The Data Protection Commission, 21 Fitzwilliam Square South, Dublin 2 D02 RD28

The Data Protection Commission also operates a helpdesk function, which is contactable at: 01 765 0100.

17. Responsibilities of Staff, Contractors and Council Members

Employees, contractors and council members working for and on behalf of the Heritage Council are responsible for adhering to all GDPR policies and guidelines contained in this Code of Practice.

Staff and council members are obliged to participate in GDPR training as it arises.

If an employee, contractor or council member is in doubt regarding their obligations, they should contact the Data Protection Officer for clarification.

Any breach of data protection policy is a serious matter and may lead to disciplinary action, up to and including dismissal.

Council members declaration of interest forms should only be accessible to authorised staff.

18. Project Planning and GDPR

The potential impact that a project or initiative might have on the privacy of individuals should always be considered. 'Data Protection Impact Assessment' (DPIA) will be integral part of all new projects i.e. data protection by design and by default. This will allow the Heritage Council to identify potential privacy issues before they arise and come up with ways to mitigate them.

Data Protection Impact Assessments describe the process for identifying risks which may arise out of the processing of personal data and how to minimise those risks.

Data Protection by design means including data privacy features in new technologies from the outset. Data Protection by default means that data privacy is automatically included in every process carried out by the Heritage Council.

Staff, contractors or council members who are engaging in new projects should carry out a Data Protection Impact Assessment. DPIA forms can be requested from the Data Protection Officer.

19. Photographs and Videos Featuring People

A person's consent (or parental consent for those under 18) is necessary when they are clearly recognisable in an image or video that you wish to share with a third party, post online or include in a hardcopy publication.

This is particularly important in the following circumstances:

- When dealing with children and minors under 18 years of age.
- Where circulation has a very wide reach and the potential for unauthorised reuse, e.g. social media.
- Where a person or persons are the focus of an image or video e.g. posed photographs.

Consent can take the form of a simple announcement that you are about to take a photograph or video and giving people the option to step aside if they do not want to be included. However, there are certain circumstances when written consent will be required.

Photographing and filming large groups at a public event

If photography or filming is taking place at a public event attended by large crowds, this is regarded as a public area so you do not need to get the permission of everyone in a crowd shot. People in the foreground of a crowd shot are also considered to be in a public area but will need to inform them of the fact and give them the option to step out of the photograph/video.

Photographing and filming individuals or small groups

Written consent should always be obtained from people whose images are the focus of the photograph or video. This also applies where a video or photograph incidentally captures passers-by in the background who are clearly identifiable.

To ensure compliance with GDPR:

- Ensure all those involved are aware/happy to be photographed or filmed.
- Obtain written permission from everyone involved.
- Obtain written permission from the parent/guardian of children or minors under 18 years of age. See Appendix B for consent form template.
- Signed consent forms must be retained and given to the Data Protection Officer.

Photographing and filming at a conference/seminar/event

To ensure compliance with GDPR:

- At the booking stage, inform them that photography/filming will be taken for social media and/or other purposes.

- At sign-in, include tick box to obtain consent for photography/filming.
- Always display a warning notice alerting delegates/attendees that photography or filming is going to take place
- Always verbally announce to those present that you will be photographing or filming, before starting to do so, so that those who have opted out may leave or move to the back of the room.
- Always offer those present the opportunity to sit somewhere they will not be photographed or filmed.
- Always inform those present of the purpose and use(s) to which images and recordings will be put.
- When children or minors are present at an event, it is recommended to use brightly coloured stickers to identify those who have not consented and ensure they are not inadvertently photographed or filmed.
- Signed consent forms must be retained and given to the Data Protection Officer.

20. Keeping Data Secure

The physical security of premises, secure network and ICT systems, and good work practices are key to data protection compliance.

Premises

Premises are to be kept secure at all times. Access and egress to and from Áras na hOidhreacht is strictly controlled by an access control and image recognition system. All visitors must sign in at reception.

For procedures in relation to out of hours work, please refer to the Heritage Council's Safety Statement.

Disposal of confidential waste

Appropriate procedures are in place for the disposal of confidential waste. Confidential waste bags are available in reception.

Small quantities of confidential waste are also shredded onsite using in-house shredding equipment and disposed of confidentially. Larger quantities are outsourced to a specialist service provider where physical destruction is supervised by a member of staff and a destruction certificate obtained.

Cyber security

The Heritage Council's servers are hosted and managed by a third-party service provider with ISO 27001 certification.

The Heritage Council's Staff Handbook contains its code of practice for employees in relation to Confidentiality (Section 5.9), E-mail and internet use (5.7) and Telephones (5.8).

The Heritage Council has put in place a suite of employee policies for Information and Communication Technology usage, and associated risk management processes to measure, manage and remediate cyber risks.

All computer systems are password protected. The ICT system is set to lock computers if they are not accessed or used upon expiration of a predefined period of time and a password is required to unlock them.

Work practices

Personal security passwords are never to be disclosed to other individuals (including other employees).

At the end of each working day, staff are required to log out of computer systems and file/lock away any records containing personal data.

Laptops and other portable devices should never be left unattended when working offsite.

Personal data should never be stored on the hard drive of a portable device. Office 365 is to be used on portable devices for the creation and storage of any documents containing personal data.

21. Changes to this policy

This policy is kept under review and is subject to change. The latest version of this policy will be available on the Heritage Council's website.

The Heritage Council will conduct an examination and review of data protection policies, procedures and risks associated with the storage, handling and protection of personal data on an annual basis. The Data Protection Officer is responsible to updating this policy as necessary.

Appendix A

Data Retention Schedule and Policy

Purpose

Article 5 (1)(c) of the GDPR states that 'Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.'

The purpose of this data retention schedule is to establish a procedure for the retention and destruction of personal data and to be transparent about how the Heritage Council processes personal data.

Scope

This data retention schedule applies to all members of staff, council members and contractors engaged by the Heritage Council.

It applies to personal data processed while discharging the duties of the Heritage Council.

Exceptions

Personal data subject to a legal investigation shall not be destroyed until the conclusion of the case.

Retention of Records

All Records must be stored in a safe, secure and accessible manner to ensure the security, integrity and confidentiality of such Records and in compliance with the Heritage Council's ICT Policy.

Records may be retained off site with third party data processors providing the third party processor has entered into a data processing agreement with the Heritage Council.

Records may only be retained for a period longer than those set out in the retention schedule if

- (a) They are subject to a legal investigation
- (b) The personal data contained within the record is removed

The Data Protection Officer must be consulted prior to any extended retention.

Retention Periods

Retention period of records containing personal data are based on the legal, regulatory and accountability obligations of the Heritage Council.

Destruction of records

Paper records should be disposed of in green shredding bags in reception for offsite shredding.

Electronic records should be deleted from shared folders, SharePoint, hard drives, mobile devices or email inboxes as appropriate.

Email “deleted” folders and desktop recycle bins should be emptied regularly to ensure that no records are accidentally retained.

Section	Records	Description	Retention Period	Record Location	Action following retention expiry	Legal basis for processing
Human Resources	Competition file	Adverts Job descriptions Application forms Referee reports Interview notes	Unsuccessful candidates: 3 years (unless a legal case is underway) Successful candidates: relevant data is kept for 100 years or 7.5 years after the death of the last surviving beneficiary, whichever is longer	HR File on R Drive for adverts, job descriptions and data of the successful 0candidate. Unsuccessful candidate data is held by recruitment agency	Destroy	GDPR Regulations Article 6(1)(a); 6(1)(b); 6(1)(c)
	Unsolicited job requests	CVs, letters	Not retained	N/A	Destroy immediately	N/A
	Candidate clearance files	Garda vetting forms, medical report, references	Relevant information is kept for 100 years or 7.5 years after the death of the last surviving beneficiary, whichever is longer	Electronic copy is held on HR File in R Drive. Hard copy files are stored in locked cabinet in Corporate Services Officer's office	Destroy	GDPR Regulations Article 6(1)(a); 6(1)(b); 6(1)(c)
	Personnel files	Name, address, date of birth, gender, ppsn, contract, terms & conditions, civil status, next of kin, dependents, pmds, probation records, job description,	Relevant information is kept for 100 years or 7.5 years after the death of the last surviving beneficiary, whichever is longer	Electronic copy is held on HR File in R Drive. Hard copy files are stored in locked cabinet in Corporate Services Officer's office	Keep record of employee's service but destroy personal data	GDPR Regulations Article 6(1)(a); 6(1)(b); 6(1)(c)
	Parental Leave	Application and record of leave	8 years but record of leave is kept for pension purposes for 100 years or 7.5	Personnel file	destroy	Parental Leave Acts 1998-2006 Section 27

			years after the death of the last beneficiary, whichever is longer			
	Force Majeure	Application and record of leave	Relevant information is kept for 100 years or 7.5 years after the death of the last surviving beneficiary, whichever is longer	Personnel file	Destroy	Parental Leave Acts 1998-2006 section 27
	Maternity Leave	Record of leave and documentation	Relevant information is kept for 100 years or 7.5 years after the death of the last surviving beneficiary, whichever is longer	Personnel file	destroy	GDPR Regulations Article 6(1)(a); 6(1)(b); 6(1)(c)
	Disciplinary cases	Oral warnings, written warnings, action taken up to and including dismissal, bullying investigations, harassment and grievance investigations	Retain record on personnel file	Locked cabinet in Corporate Services Officer's office for hard copy files and HR File in R Drive for electronic files	destroy	GDPR Regulations Article 6(1)(b)6(1)(c)
	Grievance cases	Bullying investigations, harassment claims, grievance claims	Retain record on personnel file	Locked cabinet in Corporate Services Officer's office for hard copy files and HR File in R Drive for electronic files	destroy	GDPR Regulation Article 6(1)(a); 6(1)(b); 6(1)(c)
	Legal case files		30 years	Locked cabinet or secure drive		GDPR Regulations Article 6(1)(b)6(1)(c)
	Timesheets	Record of times and days that employees work	3 years	HR System	destroy	Organisation of Working Time Act 1997

	Annual leave	Record of annual leave and public holidays taken by employees	3 years	HR System	Destroy	Organisation of Working Time Act 1997
	Pension records	records of paid and unpaid leave, timeshare patterns, absences over the lifetime of an employee's employment.	Relevant information is kept for 100 years or 7.5 years after the death of the last surviving beneficiary, whichever is longer	Locked cabinet in Corporate Services Officer's office for hard copy files and HR File in R Drive for electronic files	Review for transfer to National Archives	GDPR Regulations Article 6(1)(a); 6(1)(b); 6(1)(c)
	Sick leave records	Sick certificates; record of absences	4 years	HR System	Destroy certs and emails but keep record of absence	Organisation of Working Time Act 1997
	Occupational Health Assessments	Pregnancy Risk Assessments, Ergonomic Checks	7 years	HR File	Destroy but retain evidence of compliance	Article 9(2)(b) of GDPR and section 46, 47 and 50 of Data Protection Act 2018
Section	Records	Description	Retention Period	Record Location	Action following retention expiry	Legal basis for processing
Corporate Services	CCTV images	Images captured by cctv cameras internally and externally to the building	1 month unless required for an ongoing investigation.	CCTV System,	Destroy or overwrite	GDPR Article 6(1)(d)
	Accidents/Incidents Register	Record detailing the circumstances and nature of accidents or incidents that occur on site	10 years unless required for an ongoing investigation. Retention period for an incident relating to a child will be 2 years after their 18 th birthday	Incident book in Reception	Destroy	Safety, Health and Welfare at Work (General Applications) Regulations 1993
	Training records	Applications for courses, attendance at courses, refund of fees	Summary of relevant qualifications and training undertaken should be kept for the	HR File and on personnel file	Destroy	Article 6(1)(c)

			duration of employment plus 7.5 years			
	Externally procured services	Tender data & selection -rejected tenders	Current year plus three years	R Drive	Destroy but retain evidence of compliance with Public Procurement Guidelines	GDPR Article 6(1)(b); Article 6(1)(c)
	Externally procured services	Tender data & selection – accepted tenders. Consultant contract, performance, tax clearance, invoices & payments, general management & administration files	Current year plus three years	R Drive	Destroy but retain evidence of compliance with Public Procurement Guidelines	GDPR Article 6(1)(b); Article 6(1)(c)
	FOI & AIE requests	Contact details of requester	2 years	R Drive	Destroy but retain evidence of compliance with the Act	Freedom of Information Act 2018; European Communities (Access to Information on the Environment) Regulations 2007
	Data Subject Access Requests	Contact details of requester	2 years	R Drive & Locked unit in Corporate Services Officer's office	Destroy but retain evidence of compliance with the Act	Data Protection Act 2018 Section 91
	Board Members declaration of interest forms	Name and interest	Until superseded	R Drive & Locked unit in Corporate Services Officer's office	Destroy	Ethics Act
Section	Records	Description	Retention Period	Record Location	Action following retention expiry	Legal basis for processing
Finance	Payroll records	Contact details, Bank Details, Pension	100 years or 7.5 years after the death	Secure Drive; Finance System	Purge	National Minimum Wage Act 2000

		Details, Tax Details, Payslips; Union Membership	of last recipient, whichever is longer			
	Travel & subsistence	Contact details, Bank Details, Tax Details; Car Registration, cc and Insurance;	Current year, plus 6 years	Secure Drive; Finance System	Purge	Article 6(1)(c) - legal obligation
	Supplier Information	Processing invoices and payments to suppliers – Name and bank details	Current year, plus 6 years	Secure Drive; Finance System	Purge	Article 6(1)(c) - legal obligation
	Customer Information	Processing sales invoices and receipts.	Current year, plus 6 years	Secure Drive; Finance System	Purge	Article 6(1)(c) - legal obligation
	Heritage in Schools Payments	Processing payment to HIS Experts – Name and bank details	Current year, plus 6 years	Secure Drive; Finance System	Purge	Article 6(1)(c) - legal obligation
	Heritage Officers and Biodiversity Officers payments to Local Authorities	Name; contact details; bank details; tax details; salary details	Current year, plus 6 years	Secure Drive; Finance System	Purge	Article 6(1)(b)
Section	Records	Description	Retention Period	Record Location	Action following retention expiry	Legal basis for processing
Grants	Grant payments	Processing payment to Grantees	Current year, plus 6 years	Grants Management System (Sales Pulse; Smart Simple); Off site in storage (pre 2009)	Purge but retain record of project	Taxes Consolidation Act 1997 Section 886; GDPR Article 6(1)(b)
	Unsubmitted grant applications	Contact Name and addresses , telephone numbers, email address of applicant invoices, quotations, tax and bank, cvs of third parties, photographs,	2 years	Grants Management System (Sales Pulse; Smart Simple); Off site in storage (pre 2009)	Purge	Taxes Consolidation Act 1997 Section 886; GDPR Article 6(1)(b)

		letters of support from third parties				
	Unsuccessful grant applications	Contact Name and addresses , telephone numbers, email address of applicant invoices, quotations, tax and bank, cvs of third parties, photographs, letters of support from third parties	2 years	Grants Management System (Sales Pulse; Smart Simple); Off site in storage (pre 2009)	Purge	Taxes Consolidation Act 1997 Section 886; GDPR Article 6(1)(b)
	Successful grant applicants	Contact Name and addresses , telephone numbers, email address of applicant invoices, quotations, tax and bank, cvs of third parties, photographs, letters of support from third parties	Current year plus 6 years.	Grants Management System (Sales Pulse; Smart Simple); Off site in storage (pre 2009)	Purge but keep record of project	Taxes Consolidation Act 1997 Section 886; GDPR Article 6(1)(b)
	Unsuccessful panel members	Panel Members personal information (CVs, referees, names, contact details)	1 year	Restricted access to Network; password protection on system.	Purge	Article 6(1)(b)
	Successful panel members	Panel Members personal information (CVs, referees, names, contact details)	Life of the panel plus 1 year	Restricted access to Network; password protection on system.	Purge	Article 6(1)(b)
Section	Records	Description	Retention Period	Record Location	Action following retention expiry	Legal basis for processing
Communications	Heritage Council website, Heritage Week website,	cookies	Individual retention periods as per cookie schedule on websites	website	Automatic destruction	GDPR Article 6(1)(a) 6(1)(c)

	Heritage in Schools website, Heritage Maps website, IWTN website					
	National Heritage Week Organisers details	Name, telephone number, email address	Duration of event	Backend of heritageweek.ie and exported to R drive and mail chimp on R drive	purge	GDPR Article 6(1)(a)
	National Heritage Week Award applications	Name, telephone number, email address	Duration of event	R drive encrypted storage, survey monkey two factor authentication	Purge but keep note of winner's names	GDPR Article 6(1)(a)
	Newsletter subscriptions	Name and email address	Until user opts out	Mailchimp	purge	GDPR Article 6(1)(a)
	Heritage Council event attendees	Name and email address	Duration of event	Eventbrite and R drive, email	purge	GDPR Article 6(1)(a)
	Survey respondents	Name and email address	Duration of event	Survey monkey and R Drive	purge	GDPR Article 6(1)(a)
	Lego competition entries	Name, address, email address	Duration of event but note taken of winner's names	R Drive	purge	GDPR Article 6(1)(a)
	Journalist, photographer and media mailing lists	email address	Until user opts out	R Drive	purge	GDPR Article 6(1)(a)
	External graphic designer access to bank of photographs	Images of members of the public and stakeholders	Until superseded or contract with photographer runs out	R Drive and graphic designer's drive	purge	GDPR Article 6(1)(a)
	National Heritage Week Training Day attendees	Name, email address	Duration of event	EventBrite	purge	GDPR Article 6(1)(a)
	Photographs and video footage for promotional material	Images	Until superseded	R drive	purge	GDPR Article 6(1)(a)
	Staff photographs for ID cards and website	Images	Until superseded	R drive		GDPR Article 6(1)(a)

Section	Records	Description	Retention Period	Record Location	Action following retention expiry	Legal basis for processing
Traditional Farm Buildings Scheme	Grant Applications - successful	Name, address, contact details	As per DAFM	R Drive	Purge but retain record of project	GDPR Article 6(1)(a); 6(1)(b)
	Grant Applications - unsuccessful	Name, address, contact details	As per DAFM	R Drive	purge	GDPR Article 6(1)(a); 6(1)(b)
Section	Records	Description	Retention Period	Record Location	Action following retention expiry	Legal basis for processing
Heritage in Schools	Garda vetting disclosures and ID	Name, address, date of birth, photo ID, former addresses	Duration of panel	Secure drive	purge	GDPR Article 6(1)(c)
	Heritage specialist applications – successful applicants	CV	Duration of panel	Secure drive	Purge but keep record of panel	GDPR Article 6(1)(a); (1)(b); (1)(c)
	Heritage specialist applications – unsuccessful applicants	CV	Until end of recruitment campaign unless appeal is underway	Secure drive	purge	GDPR Article 6(1)(a); 6(1)(b); 6(1)(c)
	Tusla Child First Certificates	Name	Duration of panel	Secure drive	purge	GDPR Article 6(1)(a); 6(1)(b); 6(1)(c)
	Financial records	tax information, ppsn	1 year	Secure drive	purge	GDPR Article 6(1)(a); 6(1)(b); 6(1)(c)
	School information	Roll number, address, email addresses, phone numbers	Current year plus 1	Secure drive	purge	GDPR Article 6(1)(a)
Section	Records	Description	Retention Period	Record Location	Action following retention expiry	Legal basis for processing
Museum Standards Programme of Ireland	Assessors' communication	Name, address, email address, phone number, bank details	Until member leaves panel	Secure drive	Purge	Article 6(1)(a)
	Trainers' communication	Name, address, email address, phone number, bank details	Until member leaves panel	Secure drive	Purge	Article 6(1)(a)

	Museum communication	Name, email address	Until museum leaves programme	Secure drive	Purge	Article 6(1)(a)
Section	Records	Description	Retention Period	Record Location	Action following retention expiry	Legal basis for processing
Heritage in Schools TY Pilot	Expression of interest forms	Name, contact details, place of employment	Until end of pilot scheme	Secure drive	Purge	Article 6(1)(a)
Section	Records	Description	Retention Period	Record Location	Action following retention expiry	Legal basis for processing
All Ireland Heritage Skills Programme	Candidate applications - unsuccessful	CVs, name, contact details		R Drive	Purge	Article 6(1)(a); 6(1)(b)
	Candidate applications – successful	CVs, name, contact details		R Drive	Purge, but retain evidence of participation	Article 6(1)(a); 6(1)(b)
Section	Records	Description	Retention Period	Record Location	Action following retention expiry	Legal basis for processing
External personnel (contractors)	Contracts	Name, address, phone number, email address	current year plus 6 years	Hard copies of procurement/consultant files that are internally sensitive are to be stored in a locked filing cabinet. Electronic files should be stored on a secure Drive	Purge	Article 6(1)(b)
Section	Records	Description	Retention Period	Location where record is held	Action following retention expiry	Legal basis for processing

Heritage in Education Policy Development Officer	Pilot project	Name, email address, place of employment	Until end of project	Secure drive	Purge but keep record of school's participation in project	Article 6(1)(a)
	Consent forms	Name	Until end of project	Secure drive	Purge but keep record of school's participation in project	Article 6(1)(a)
Section	Records	Description	Retention Period	Location where record is held	Action following retention expiry	Legal basis for processing
Planning	Correspondence	Name, address	As per IT policy, 1 year	email	Anonymise but retain content	Article 6(1)(a)

Appendix B

Template Consent Form for Filming and Photography

Consent Form for Filming and Photography

Photographer/Videographer Information	
Name:	
Photo/Shoot Title:	
Location:	
Date:	
Photographed/Recorded Person's Information	
Name:	
Are you over 18?	

Terms and Conditions of Use

- I hereby consent to the unrestricted use by the Heritage Council and those acting with its permission to use any images of me captured in video footage and/or photographs created today in any media (whether now known or hereafter de-vised), throughout the world, and for any purpose (excluding defamation) which may include, among others, advertising, promotion and marketing. The Heritage Council may also delegate, subcontract or assign such consent to any third party without consideration.
- I waive any right to inspect or approve the finished footage, imagery, advertising copy, text, or other printed matter that may be used in conjunction therewith.
- My image(s) will be held in accordance with GDPR (General Data Protection Regulation).
- Images of me captured in video footage/photographs will be the copyright of the Heritage Council and any other intellectual property which arises in the recordings will also belong to the Heritage Council.

Photographed/Recorded Person's Signature:

Name of Parent/Guardian if Person is under
18 years of age:

Signature of Parent/Guardian if Person is
under 18 years of age:

Appendix C

Template

Filming/ Photography Location Warning Notice



Location Warning Notice

Filming/Photography Taking Place Here

Please be advised that filming and/or photography will be taking place here in this area between the hours of [insert hours] on [insert date]

If you do not wish to be appear in any images captured, please

[Avoid this area at these times] *

[Sit at the back of the room] *

[Tell us so we can take appropriate steps to ensure you are not included] *

The photographs/film will be used by the Heritage Council for [insert details]. They may also be used by The Heritage Council for promotional and communication purposes e.g. social media, publications, Heritage Council website, etc.

[Insert other purpose as applicable] **

