

Privacy notice: collection of impact evidence for REF 2029

Contents:

1. About the University of Reading and the REF	2
2. University of Reading’s Data Controller	2
3. Purpose of processing	3
4. Lawful basis of processing	3
5. Categories of personal data we collect	3
7. Recipients and data sharing.....	4
8. International transfers	5
9. Retention periods	5
10. Your data protection rights	5
11. Is provision of data mandatory?	5
12. Automated decision making	6
13. Security measures.....	6
14. How to get in touch.....	6

1. About the University of Reading and the REF

Who we are: The University of Reading is collecting **impact evidence** (e.g. testimonials, letters, metrics) to develop and audit **Impact Case Studies** for **REF 2029**, the UK-wide research assessment [\[2029.ref.ac.uk\]](https://2029.ref.ac.uk).

Why we use your data: To prepare, submit and evidence our REF impact materials—an activity carried out **in the public interest** for accountability and funding of UK research.

What we collect: Names, job titles, organisational affiliation, contact details (where needed for audit), and the content of impact evidence you provide. We avoid sensitive data unless clearly necessary and safeguarded.

Who sees it: Internal REF teams; external assessors and panels under confidentiality; **UKRI/Research England** (REF managers). Published case studies may include **your name and job title** but not contact details or full evidence files [\[2029.ref.ac.uk\]](https://2029.ref.ac.uk).

Your rights: You can ask us for access, correction, objection (where applicable), or to limit use. You also have a right to complain to the **Information Commissioner's Office:** [Make a complaint](#).

2. University of Reading's Data Controller

Data Controller: The University of Reading

Contact details for the Data Protection Officer: Information Management and Policy Services, Whiteknights House, Shinfield Road, Whiteknights, READING, Berkshire, RG6 6UR, United Kingdom.

Email: imps@reading.ac.uk

Phone: 0118 378 8981

3. Purpose of processing

We process personal data to:

- Develop, quality-assure and submit **Impact Case Studies** and related impact evidence to **REF 2029**, including pre-submission peer review and audit preparation [2029.ref.ac.uk].
- Provide transparency and accountability for public investment in research and to inform research funding decisions.
- Manage requests from REF panels/assessors for corroboration during audit.

4. Lawful basis of processing

Our lawful basis is **Article 6(1)(e) UK GDPR – public task**: processing is necessary to perform a task carried out in the public interest and/or under official authority (participation in the national REF exercise and associated accountability).

Where impact evidence contains **special category data** (e.g. health information) and its inclusion is strictly necessary, we rely on:

Article 9(2)(g) reasons of substantial public interest. This is qualified by Part 2 of Schedule 1 of the Data Protection Act 2018 – Statutory and government purposes as laid down in our University Charter, OR

Article 9(2)(j) – processing necessary for scientific or historical research purposes, subject to **Article 89(1)** safeguards (data minimisation, access controls, pseudonymisation where possible).

We document the specific lawful basis per processing activity and apply research safeguards, in line with data protection transparency requirements.

5. Categories of personal data we collect

- **Identification and role:** Name, job title/role, organisational affiliation.

- **Contact details:** Business email/phone **only where needed** for audit/corroboration by REF panels.
- **Evidence content:** Letters/testimonials, statements, metrics, documents and quotes supplied to corroborate impact.

Sources of personal data

Personal data are obtained:

- **Directly from you** when you provide impact evidence or agree to act as a corroborating contact.
- **Indirectly**, from publicly available sources (e.g., published reports, websites) where relevant to impact corroboration.

7. Recipients and data sharing

We may share personal data with:

- **UKRI/Research England (REF managers)** via secure REF systems for submission and audit. Some materials may be shared with other UK funding bodies (SFC/HEFCW/DfE NI) for analysis relating to research funding.
- **REF panels and assessors**, under confidentiality, for the sole purpose of assessment and audit (corroborating sources are **not** published).
- **Internal reviewers** and approved external peer reviewers supporting case study quality assurance prior to submission.

Publication:

REF will publish outcomes and case studies on public webpages. Published materials may include **textual references to you (e.g. name, job title)** and quotes; **corroborating evidence files and contact details will not be published**.

If necessary, due to **commercial sensitivity or security**, we may mark case studies “not for publication” or submit redacted versions [2029.ref.ac.uk].

8. International transfers

We do **not** routinely transfer REF impact evidence outside the UK. If any transfer is necessary (e.g. to a service provider outside the UK), we will apply appropriate safeguards required by the **UK GDPR** (including by way of adequacy decisions or standard contractual clauses/International Data Transfer Addendums).

9. Retention periods

We retain working evidence files and published case study text in the following ways:

- **Working evidence files and corroborating contacts:** Retained until the conclusion of REF 2029 audits and any subsequent verification activities, then reviewed and either securely deleted or archived with access controls, in line with research safeguards (Article 89) and our records policy.
- **Published case study text:** May be kept indefinitely on public websites managed by UKRI/REF [2029.ref.ac.uk].

10. Your data protection rights

Subject to applicable research and assessment exemptions, you have rights to:

- **Access** your personal data; **rectify** inaccuracies; **restrict** processing; and **object** to processing under Article 6(1)(e) in certain circumstances.
- **Complain** to the **Information Commissioner's Office (ICO)**: Wycliffe House, Water Lane, Wilmslow, SK9 5AF; 0303 123 1113; www.ico.org.uk.

11. Is provision of data mandatory?

Providing impact evidence or acting as a corroborating contact is **not a statutory requirement**. However, if you decline to provide information, we may be **unable to reference or corroborate** certain impact claims in our REF submission.

If you prefer **not** to have your **name, organisation or job title** disclosed in a published case study, we can use **an anonymised attribution** (e.g., “a senior manager”), while still providing corroborating evidence to REF via secure systems. Please tell your academic contact or the Impact Team.

12. Automated decision making

We do **not** use automated decision making (including profiling) in processing impact evidence for REF.

13. Security measures

We apply **data protection by design and by default**. We will apply appropriate technical and organisational security measures, including role-based access, secure storage, encryption, and minimisation; corroborating evidence is shared **only via secure channels** and accessible to authorised assessors.

Appendix 1 (page 7) includes Impact Case Study redaction options outlines ways in which we can redact your data before publication.

14. How to get in touch

Impact Team: Dr Lisa Lazareck-Asunta, Head of Impact

Email: l.j.lazareck-asunta@reading.ac.uk (for impact case study queries, including confidentiality/redaction requests).

Information Management and Policy Services (Data Protection Office) University of Reading: imps@reading.ac.uk (for data rights and privacy queries).

Appendix 1: REF Impact Case Study redaction options

You may choose to redact information from REF Impact Case Studies. If you would like to discuss your redaction options in more depth, please contact the Head of Impact, [Dr Lazareck-Asunta](#).

Level	Description	Internal Process	Evidence	REF2029 review by	Publish on REF website	Notes
Security Sensitive	Case study based on or containing security sensitive information	Reviewed only by persons with security clearance	Only appropriate evidence is to be supplied and stored by those with security clearance only.	Only by those with appropriate security clearance	No	Needs to be highlighted to the REF team through formal reporting process before submission date (TBC)
Redaction (1)	Case study contains commercially sensitive information that cannot be published or reviewed by the whole REF2029 sub-panel	Reviewed only by persons with security clearance	Sensitive evidence to be directly transferred to Secure SharePoint by author and any sensitive documents highlighted to impact leads.	May identify specific panel members who should not have access to, or should have access only to the redacted versions	No	Author must give clear indication of who should not see the case study as soon as possible to ensure appropriate processes are put into place

Redaction (2)	Case study contains commercially sensitive or third-party personal data information that cannot be published, but can be reviewed by REF2029 sub-panel members	Reviewed only by persons identified as appropriate and marked as sensitive	Sensitive evidence to be directly transferred to Secure SharePoint by author and any sensitive documents highlighted to impact leads.	May identify specific panel members who should not have access to, or should have access only to the redacted versions	No	Author must give clear indication of who should not see the case study as soon as possible to ensure appropriate processes are put into place
Redaction (3)	Case study contains small amounts of sensitive data which cannot be viewed by REF2029 sub-panel members, but the whole case study can be published with redaction	Normal review process takes place with reviewers aware of sensitive sections	Evidence may be transferred onto a Secure SharePoint by a Research Administrator. Any sensitive documents should be clearly identified.	All sub-panel members can review case study	Redacted version published	Redacted versions suitable for publication to be submitted by - date TBC
Partially Redacted	Case study contains small amounts of sensitive data which can be viewed by REF2029 sub-panel members, but the whole case study can be published with redaction	Normal review process takes place with all reviewers aware of sensitive sections	Evidence may be transferred onto Secure SharePoint by a Research Administrator. Any sensitive documents should be clearly identified.	All sub-panel members can review unredacted case study	Redacted version published	Redacted versions suitable for publication to be submitted by - date TBC

Standard Case Study	Case study contains no commercially sensitive or potentially inappropriate intellectual property	Normal review process takes place	All case study information stored securely within our research information systems and SharePoint.	All sub-panel members can review unredacted case study	Full version published	All case studies must be reviewed by governance team for GDPR compliance
----------------------------	--	-----------------------------------	--	--	------------------------	--

Version control

Version	Keeper	Reviewed	Approved by	Approval date
1.0	Ethics COP	Annually	Ethics COP	1 June 2026