Data Protection & Research Data Handling Policy

Athronydd Research and Consulting

Applies to: All research, consulting, filming, evaluation and co-production work involving **personal data**, including that of children, young people, school staff, performers and contributors.

---

1. Purpose

This policy explains how Athronydd Research and Consulting ("Athronydd") meets its responsibilities under the **UK General Data Protection Regulation (UK GDPR)** and **Data Protection Act 2018** when collecting, storing, using and sharing personal data — including special category data — during research and project delivery.

2. Scope

This policy applies to:

- **Research and evaluation** with learners, educators, youth professionals or parents
- **CPD filming or training content** involving actors/contributors
- **Schools and youth settings** where any personal data is collected or processed
- Any **recordings, transcripts, survey responses, interviews**, or images linked to a person

3. Key Definitions

- **Personal data:** Any information that identifies a living individual (e.g., name, contact details, voice, image, ID numbers).
- **Special category data:** Sensitive personal data, such as health, race/ethnicity, religion, sexuality, political views.
- **Processing:** Anything done with data — collecting, storing, analysing, sharing or deleting.
- **Data subject:** The person the data relates to.

- **DPIA:** A **Data Protection Impact Assessment**, required where processing may pose a high risk (e.g. involving children, special category data, or sensitive filming).

4. Our Commitments

Athronydd commits to:

- Collecting only the **minimum data necessary** for each purpose
- Being transparent with participants and contributors
- Ensuring data is stored **securely** and only accessed by authorised personnel
- Retaining data **only as long as needed**
- Respecting data subject **rights** (see Section 10)
- Completing **DPIAs** when required
- **Not selling** or exploiting personal data

5. Roles & Responsibility

- **Joint Data Controllers (default):** CSM and MK (Partners)
- **DPO Contact:** [Insert DPO contact if appointed, or note “No statutory DPO required under current scale”]
- **All Partners and Associates**: responsible for secure handling, recording, anonymisation, and compliance with this policy

Where Athronydd works with a **school or commissioning body**, we may be a **joint controller** or a **data processor** depending on project design. This will be agreed in writing.

6. What Data We Collect (Examples)

Activity	Data Collected	Special Category?	Notes
Surveys	Name (optional), age/school year, views	Possibly	Often anonymised or pseudonymised
Interviews	First name, voice/image (if recorded), opinions	Possibly	Written consent or assent + parent consent if U16
Filming CPD	Contributor name, voice/image, signed release	No	Adults only; release form required

Evaluation data	Age, experience, quotes, responses	Possibly	Minimise personal detail
Safeguarding	Incident notes, concern details	Yes	Shared with DSL only; securely stored

7. Lawful Basis for Processing

Athronydd uses one or more of the following **UK GDPR lawful bases** depending on context:

Purpose	Lawful Basis	Notes
Research (adults)	**Consent** (Article 6.1.a) or **Public task** (6.1.e)	Consent used when participation is voluntary
Children & young people	**Consent** + **assent**	Parental consent if required by setting
Safeguarding	**Vital interests** (6.1.d) or **Legal obligation** (6.1.c)	Shared with DSLs or statutory services
Special category data	**Explicit consent** (Article 9.2.a) or **substantial public interest** (9.2.g)	For e.g., ethnicity, health, SEND — only if necessary

> Consent is always **freely given, informed, specific and revocable** (except where overridden by law).

8. Information Provided to Data Subjects

Before collecting data, Athronydd provides:

- An **Information Sheet** (age-appropriate)
- A **Consent Form** (and where relevant, an Assent Form for CYP)
- Contact details for questions or complaints
- Clear explanation of:
    - What data is collected
    - How it will be used and shared
      How long it will be kept
    - Whether it will be anonymised or pseudonymised
    - Rights under UK GDPR

9. Data Storage & Security

- Personal data is stored on **encrypted, password-protected** devices and/or cloud platforms (e.g., Microsoft 365 or Google Workspace with 2FA).
- Audio/video files are **labelled by code**, not names.
- Hard copies (e.g., consent forms) are stored securely and destroyed after retention period.
- Access is restricted to project team members on a **need-to-know basis**.
- Transfers use **encrypted channels** (not public links or open drives).
- Personal devices must **not** be used to store or transfer personal data.

10. Data Subject Rights

Under UK GDPR, all individuals have the right to:

- **Be informed** about data use
- **Access** their data
- **Rectify** incorrect data
- **Erase** data ("right to be forgotten")
- **Restrict** or object to processing in certain contexts
- **Complain** to the Information Commissioner's Office (ICO)

Athronydd will respond to any Subject Access Request (SAR) **within 30 calendar days** and explain any lawful reason for withholding data (e.g., if disclosure risks another person's privacy).

11. Retention Periods

Data Type	Typical Retention	Notes
Research data (anonymised)	Up to 5 years	For audit, reporting, or replication purposes
Personal contact data	Until project end + 6 months	Then deleted or anonymised
Signed consent forms	Up to 6 years (adults) or until child is 25	In line with WG/school guidance
Safeguarding records	Until child is 25 (or 6 years post-closure)	Follow host school/local authority policy
Financial records	6 years	For audit compliance

12. Data Protection Impact Assessments (DPIAs)

Athronydd conducts a DPIA when data processing involves:

- Children or vulnerable groups
- Special category data
- Filming, recording or identifiable images
- New technologies or third-party platforms
- High risk of harm if breached

DPIAs include data flows, risk assessment, mitigations, lawful basis, and consultation (if required). Templates available on request.

13. Third Parties & Sharing

Athronydd may share data with:

- **Schools or host settings**, where necessary for pastoral care, safeguarding or project delivery
- **Commissioning bodies** (e.g., Welsh Government) — only anonymised or pseudonymised data unless otherwise agreed
- **Local Authority or Police**, if required by safeguarding law

Athronydd **does not** sell or share personal data with commercial advertisers, social platforms, or external analytics tools without consent.

14. International Transfers

Athronydd stores data within the UK or EEA wherever possible. If an external processor is used (e.g., transcription service, secure cloud storage outside the UK), appropriate **Standard Contractual Clauses (SCCs)** or transfer risk assessments are used in line with ICO guidance.

15. Breaches & Incident Response

Any data breach (accidental loss, disclosure, or unauthorised access) will be:

- Logged and assessed for risk
- Escalated to the ICO if it poses a risk to individuals' rights
- Notified to affected data subjects where required
- Athronydd will document the breach and steps taken to mitigate harm.

16. Training & Governance

- Both Partners complete annual **data protection refreshers**
- All associates working with identifiable data are briefed and sign confidentiality agreements
- This policy is reviewed **annually** or after any incident/change in law

17. Version Control

Version	Date	Author	Summary
1.0	26/07/2025	Athronydd	Initial issue

Sign-off:

- **Partner 1:**  Date: 27/07/2025
- **Partner 2:**  Date: 27/07/2025