Data Protection Policy

Seagull Media House CIC

Last Updated: 2nd December 2025

Approved by the Board of Directors

---

1. Introduction

Seagull Media House CIC ("the Company") is committed to protecting the privacy, rights, and personal data of all individuals whose information it processes. This policy outlines how the Company collects, stores, uses, shares, and protects personal data in accordance with UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and all applicable privacy legislation.

This policy applies to all Directors, staff, volunteers, contractors, and anyone handling data on behalf of the Company.

---

2. Scope of This Policy

This policy covers personal data relating to:

- Participants
- Employees, freelancers, and volunteers
- Applicants for programmes, casting, or employment
- Email subscribers
- Members of the public interacting with the Company
- Individuals appearing in media or recordings where consent is required

It applies to data collected through:

- Online forms, applications, and email sign-ups
- Paper documents and physical records

- Filming, photography, and media capture

  Events, workshops, productions, and training activity

---

3. Data Controller

The Company is the Data Controller.

Seagull Media House CIC

117 Rectory Lane

Chelmsford

CM1 1RF

United Kingdom

---

4. Data Protection Lead

The Company appoints a Data Protection Lead responsible for overseeing compliance with this policy.

This is a role-based designation and not a statutory Data Protection Officer.

Responsibilities include:

- Ensuring compliance with UK GDPR
- Monitoring data practices and reporting breaches
- Managing data access requests
- Maintaining records of processing activity

---

5. Legal Basis for Processing

The Company processes personal data under one or more of the following legal bases:

- Consent – individuals provide clear consent for specific purposes.

  Legitimate Interests – processing is necessary for the Company's operations and does not override individuals' rights.

- Contractual Necessity – required to fulfil agreements with staff, freelancers, participants, or applicants.

- Legal Obligation – required by safeguarding, employment law, HMRC, or regulatory compliance.

Where data is processed based on consent, individuals may withdraw consent at any time.

---

6. Categories of Data Collected

The Company may collect:

- Contact information (name, email, phone)
- Demographic information (age, postcode, access needs)
- Media and photography consent data
- Employment and application information
- Safeguarding information when legally required

The Company does not collect Special Category Data unless:

- Consent is explicit; and
- It is necessary for safeguarding, access needs, or legal compliance.

---

7. Data Storage and Security Measures

Data may be stored on:

- Personal devices used for Company business

- Company-owned devices
- Secure hard-copy storage

Third-party digital systems (e.g., CRM or email systems)

All storage must follow these rules:

- Devices must be password-protected
- Sensitive data must be encrypted where possible
- Hard-copy records stored in locked, secure locations
- Access restricted to authorised personnel only

---

8. Sharing Data With Third Parties

Data may be shared with:

- Partners delivering Company projects
- Funders requiring anonymised reporting
- Legal bodies where required by law
- Third-party processors (e.g., email platforms, cloud storage)

The Company does not sell personal data.

Any third-party processors must comply with UK GDPR.

---

9. Data Retention and Disposal

Personal data will only be retained for as long as necessary.

A separate Data Retention Schedule defines specific timeframes.

Data must be securely destroyed when no longer required.

---

10. Rights of Data Subjects

Individuals have the right to:

Access their data

- Request rectification or deletion
- Withdraw consent
- Restrict processing
- Object to processing
- Request data portability

Requests should be submitted to the Data Protection Lead.

---

11. Data Breach Procedure

Any suspected data breach must be reported to the Data Protection Lead immediately.

If a breach is likely to risk individual rights and freedoms, the ICO will be notified within 72 hours.

---

12. Policy Review

This policy will be reviewed annually or following significant organisational, legal, or operational changes.

---

13. Approval

Last Reviewed: 2nd December 2025

Next Review Due: 2nd December 2026

Approval from Director(s):

Name: Kieran Lomas

Signature: Signed by: 9C652818DA9D4F8...

Approval from Advisors:

Name: Marina Oliveira

Name: Jasmine Woodard-Harris

Name: Josh Jenkins

Signatures:

DocuSigned by: EF309D651F134DB...

Signed by: D832D71EA4ED446...

Signed by: 3B59D55C78DD435...