



information and Data Sharing Policy

Organisation: The Footlights Group Ltd / Footlights Theatre Schools Ltd

Effective From: 18/09/20005

Next Review: 26 June 2027

Version: 1.0

1. Purpose

This policy outlines how Footlights franchisees must collect, store, use, and share information in a way that complies with data protection law and supports the safeguarding and wellbeing of students, staff, and volunteers.

Franchisees are independently responsible for ensuring compliance with data protection regulations within their own business operations.

2. Legal Framework

This policy is aligned with:

- **UK General Data Protection Regulation (UK GDPR)**
 - **Data Protection Act 2018**
 - **Children Act 1989 and 2004**
 - **Working Together to Safeguard Children (2023)**
 - **Keeping Children Safe in Education (2023)**
-

3. Scope

This policy applies to:

- Student and parent information
- Staff and volunteer data
- Safeguarding and incident reports
- Health and medical details
- Photography, video, and social media content



- Communications (written, digital, or verbal)
-

4. Responsibilities

Franchisees must:

- Appoint a person responsible for data protection within their school
- Ensure staff and volunteers understand their responsibilities
- Store data securely (digitally and physically)
- Use only secure communication systems (e.g., password-protected email)
- Follow this policy and UK data protection laws at all times

The Footlights Group Ltd and Footlights Theatre Schools Ltd do not accept liability for data breaches or failures to comply with this policy within individual franchises.

5. Lawful Basis for Collecting Information

Franchisees must have a lawful reason to collect and process data, including:

- **Consent** (e.g. media permissions)
 - **Legal obligation** (e.g. safeguarding or health and safety)
 - **Contractual requirement** (e.g. enrolment)
 - **Vital interests** (e.g. in a medical emergency)
 - **Public task** (e.g. sharing with social services or police)
-

6. Data Storage and Retention

- Personal data must be stored securely:
 - Physical documents in locked cabinets
 - Digital files in encrypted or password-protected systems
 - Cloud based with passwords



- Records should only be retained for as long as necessary:
 - Student records: typically **6 years** after leaving
 - Safeguarding concerns: **until the subject turns 25**
 - DBS certificates: **not kept beyond 6 months**
 - All data disposal must be secure (shredding or permanent deletion)
-

7. Data Sharing

Data should only be shared when:

- There is a **clear and lawful reason**
- It is necessary to protect a child's **safety or wellbeing**
- You are sharing with a **trusted partner agency** (e.g. school, social care, police)
- You have obtained **parental or individual consent**, where appropriate

Franchisees **must not**:

- Share data via unsecured methods (e.g. personal WhatsApp or public email)
 - Discuss personal matters in public spaces
 - Share data with third parties for marketing without explicit consent
-

8. Safeguarding and Duty to Share

In safeguarding cases, the **duty to protect a child overrides confidentiality**.

Information may be shared **without consent** if:

- A child is at risk of harm
- A crime has been or may be committed
- Delaying information-sharing could place someone at risk

Always record:

- What was shared
- Why it was shared



- With whom it was shared
 - Date and time of the disclosure
-

9. Subject Access Requests (SARs)

Under UK GDPR, individuals (or parents on behalf of children) have the right to:

- Access the data you hold about them
- Request correction or deletion

Franchisees must respond to SARs **within one calendar month**. Legal exemptions may apply (e.g., safeguarding investigations).

10. Breaches of Data Protection

If a data breach occurs:

- Contain and secure the data immediately
 - Inform the affected individual(s)
 - Record the breach and actions taken
 - Report to the Information Commissioner's Office (ICO) **within 72 hours** if the breach is significant
-

11. Staff Responsibilities and Training

All staff and volunteers must:

- Follow this policy and local procedures
 - Complete regular data protection and safeguarding training
 - Know how to report a concern or breach
-

12. Review and Monitoring

Franchisees must:



- Review this policy **annually**
- Keep logs of data breaches or complaints
- Audit their data handling procedures regularly