



CONFIDENTIALITY & INFORMATION HANDLING POLICY

CAA Accreditation & Compliance Policy

Football Development East Limited

Version	1.1
Issue date	30th September 2026
Next scheduled review	31st December 2027
Policy owner	Jon Haines
Senior role	Owner / Senior Responsible Person
Applies to	All FDE staff, workers, coaches, volunteers, contractors and relevant partners

FDE POLICY POSITION

This policy forms part of FDE's safeguarding, welfare and operational governance framework. It is intended to be applied in practice, not simply retained as a compliance document.



1. Purpose

FDE holds information that children, families, staff and partners are entitled to expect will be handled sensitively. Confidentiality means information is accessed, used and shared only for a legitimate purpose by people who need it. Confidentiality is not absolute: information may and must be shared where necessary to safeguard a child, protect life, comply with law or meet another lawful duty.

2. Children's personal information

- Name, date of birth, address and contact details
- Parent/carer and emergency-contact details
- Medical conditions, allergies, medication and disability/SEND information
- Dietary, communication, behavioural, welfare and support information
- Safeguarding concerns, disclosures and referrals
- Attendance, booking, collection and participation records
- Accident, incident and injury information
- Photographs, video, performance reports and development records where identifiable

3. Parent/guardian information

- Names, addresses, telephone numbers and email addresses
- Emergency-contact and authorised-collection information
- Booking, payment and account information
- Communications, complaints, consents and preferences
- Information supplied about family circumstances where relevant to safeguarding, welfare or service delivery

4. Staff and volunteer information

- Identity, address, contact and emergency-contact information
- Application, employment history, references and interview records
- Right-to-work, DBS/PVG/AccessNI and other vetting information
- Qualifications, training, first-aid and safeguarding records
- Payroll, contractual, attendance and deployment information
- Supervision, performance, conduct, complaint, disciplinary and safeguarding information

5. Activity and operational records

- Registers and attendance records
- Session plans, risk assessments and venue checks



- Accident, incident, near-miss and medication records
- Individual Healthcare Plans and Individual Support Plans
- Behaviour/welfare notes and authorised collection records
- Performance or coaching reports
- Photographic/video consent and media records
- Complaints, feedback and investigation records

6. Staff and volunteer responsibilities

- Access information only where required for the role.
- Do not discuss children, families or colleagues in public or with people who do not need the information.
- Do not use confidential information for personal purposes or curiosity.
- Use approved systems and accounts; protect passwords and devices.
- Check identity and recipient details before disclosing information.
- Do not promise a child absolute secrecy where safeguarding may require information to be shared.
- Report accidental disclosure, loss, inappropriate access or suspected breach immediately.
- Return or securely dispose of FDE information when the engagement ends.

7. Storage

Electronic confidential information will be stored on approved access-controlled systems with permissions appropriate to role. Particularly sensitive safeguarding, medical and recruitment information will have restricted access. Paper records will be stored securely when not in active use. Records will not be left visible in vehicles, public areas or unattended venues.

8. Sharing

Before sharing confidential information, staff should consider identity, purpose, necessity, proportionality, lawful basis and the minimum information required. Routine information may be shared with authorised parents/carers and relevant staff. Sensitive information will be shared on a need-to-know basis. Safeguarding information may be shared with children's social care, police, LADO, governing bodies or other relevant agencies without consent where necessary and lawful to protect a child.

9. Electronic communication

Confidential information should be sent using approved channels. Group messages must not expose recipients' contact details unnecessarily. Highly sensitive information should not be placed in informal group chats. Images and documents must not be forwarded outside their intended purpose.



10. Requests from parents and third parties

A parent does not automatically have an unrestricted right to every record concerning a child or another person. Requests for personal data will be referred to the Data Protection Lead and considered under data-protection, safeguarding and confidentiality requirements.

11. Breaches

A confidentiality breach will be reported immediately to FDE management/Data Protection Lead. FDE will contain the breach, assess risk, preserve evidence, notify relevant people or authorities where required and take proportionate corrective or disciplinary action.

12. Relationship with other policies

This policy should be read with FDE's Safeguarding Children Policy, Data Protection & UK GDPR Policy, Staff Code of Conduct, Complaints Procedure and records-retention arrangements.

Approval and review

This policy was issued on 30th September 2026. It will be kept under review and may be revised sooner following legislative, regulatory, safeguarding, operational or CAA requirements. The next scheduled formal review is 31st December 2027.

Name	Jon Haines
Senior job title	Owner / Senior Responsible Person
Signature	
Date signed	30 th September 2026

Contact: info@fdeonline.co.uk | 0330 043 9456 | 128 City Road, London EC1V 2NX