DATA ACCESS DECISION SIMULATOR

EduConnect Ghana - DevOps Security Assessment

Organization: EduConnect Ghana Ed-Tech Platform

Users Impacted: 50,000+ Students

Report Date: Monday, February 9, 2026

Assessed By: DevOps Engineering Team

Classification Framework: PUBLIC | INTERNAL | CONFIDENTIAL

SECURITY NOTICE: This report contains decisions on data access requests involving CONFIDENTIAL student information. All decisions are made in accordance with Ghana Data Protection Act (2012), Principle of Least Privilege, and EduConnect's Data Classification Policy.

EXECUTIVE SUMMARY

As the DevOps Engineer responsible for infrastructure security and data governance at EduConnect Ghana, I have reviewed three data access requests received on Monday morning. These requests involve varying levels of data classification (PUBLIC, INTERNAL, CONFIDENTIAL) and different stages of the data lifecycle (Use, Share, Destroy).

This report provides comprehensive decision analysis for each request, examining them through the lens of:

- Data Classification Policy compliance
- Principle of Least Privilege
- Ghana Data Protection Act (2012) requirements
- Data lifecycle management best practices
- Infrastructure security and operational risk

All three requests require either denial or conditional approval with significant safeguards. None can be approved as-submitted without violating our security policies or legal obligations.

Request	Requestor	Decision	Risk Level
Marketing Campaign (Full Student Database)	Sarah Owusu Marketing Manager	CONDITIONAL APPROVAL	HIGH
Analytics Partnership (AWS Database Access)	David Mensah Head of Product	DENY	CRITICAL
Account Deletion (Right to be Forgotten)	Comfort Asante Customer Support	APPROVE (with conditions)	MEDIUM

REQUEST 1: MARKETING CAMPAIGN DATABASE ACCESS

Field	Details
Requestor	Sarah Owusu, Marketing Manager
Department	Marketing
Request Date	Monday, February 9, 2026
Urgency	Campaign starts Friday (3 days)
Data Requested	Full student database: names, emails, phone numbers, course enrollments
Current Access Level	INTERNAL access only
Purpose	New referral campaign launch

Data Classification Analysis

Requested Data Elements and Classification Levels:
• **Email Addresses:** CONFIDENTIAL (Personal Identifiable Information - PII)
• **Phone Numbers:** CONFIDENTIAL (PII - not requested but mentioned as "full database")
• **Student Names:** INTERNAL (Personally identifiable but lower sensitivity)
• **Course Enrollments:** INTERNAL (Academic records, privacy-sensitive)

Policy Violation: Request includes CONFIDENTIAL data (emails, phone numbers) but Sarah only has INTERNAL access level. Granting "full database" access would violate classification policy and expose 50,000+ students' PII without proper authorization or safeguards.

OFFICIAL DECISION FORM - REQUEST #1

DECISION	**CONDITIONAL APPROVAL**
Lifecycle Stage	**USE → SHARE (Internal use transitioning to external marketing channel)**
Risk Assessment	**HIGH - Involves bulk export of 50,000+ CONFIDENTIAL records**
Compliance Status	**Requires Ghana DPA consent verification before marketing use**

Justification (DevOps Security Perspective)

Why CONDITIONAL APPROVAL (Not Outright Approval):

1. Principle of Least Privilege Violation:
The request asks for "full student database" which violates least privilege. Marketing needs only the MINIMUM data required for the referral campaign. As DevOps, I cannot grant blanket database access when a filtered, anonymized subset would suffice.

2. Data Lifecycle Stage Analysis:

This represents a transition from USE (data stored for educational purposes) to SHARE (marketing communications). Under Ghana DPA, we must verify that students consented to marketing use when they registered. Our consent management system logs show only 68% of students opted into marketing communications.

3. Infrastructure Security Risk:
Exporting 50,000 records to Marketing's systems (likely Google Sheets or Excel) creates several risks:
- Data at Rest: Marketing laptops may lack full-disk encryption
- Data in Transit: Email attachment or unsecured file transfer
- Access Control: No audit trail once data leaves our secured AWS environment
- Retention: Marketing may retain data indefinitely without lifecycle controls

4. Legal Compliance (Ghana Data Protection Act):
Section 15 of Ghana DPA requires:
- Explicit consent for marketing communications
- Purpose limitation (data collected for education, now used for marketing)
- Right to object to direct marketing

We cannot legally send marketing emails to all 50,000 students without verified consent.

5. Operational Alternatives Exist:
As DevOps, I can provide a much safer alternative:
- Create a secure, read-only database view with ONLY marketing-consented students
- Implement API-based access rather than bulk export
- Use our email service provider's (ESP) API to upload contacts securely
- Enable automatic de-duplication and unsubscribe handling

Mandatory Safeguards for Conditional Approval

Before granting access, the following safeguards MUST be implemented:

1. Data Filtering and Minimization:

```
CREATE VIEW marketing_approved_students AS
SELECT student_id, first_name, email
FROM students
WHERE marketing_consent = TRUE
AND email_verified = TRUE
AND opt_out_date IS NULL
AND account_status = 'active';
```

This reduces exposure from 50,000 to ~34,000 consented students (68% consent rate).

2. Secure Data Transfer Method:
- NO email attachments or Google Drive sharing
- USE: SFTP with AES-256 encryption to Marketing's designated folder
- OR: API integration with our approved ESP (e.g., Mailchimp, SendGrid)
- IMPLEMENT: One-time download link with 24-hour expiration

3. Access Control and Audit Logging:
- Create temporary IAM role for Sarah with read-only access to marketing view
- Enable CloudTrail logging for all data access
- Auto-revoke access after 7 days
- Log every row accessed with timestamp and IP address

4. Data Handling Agreement:
Sarah must sign a Data Processing Agreement (DPA) that includes:
- Data retention limit: Delete after campaign completion (max 30 days)

- Storage requirements: Encrypted laptop, no personal devices
- Sharing prohibition: Cannot share data with third parties
- Breach notification: Report any data exposure within 24 hours

5. Technical Implementation (DevOps Tasks):

```
# Step 1: Create read-only database view (see above)
# Step 2: Generate secure export
psql -d educonnect -c "\COPY marketing_approved_students TO '/tmp/marketing_export.csv' CSV
HEADER"
# Step 3: Encrypt file
gpg --symmetric --cipher-algo AES256 /tmp/marketing_export.csv
# Step 4: Upload to secure S3 bucket with pre-signed URL
aws s3 cp /tmp/marketing_export.csv.gpg s3://educonnect-secure-transfers/
aws s3 presign s3://educonnect-secure-transfers/marketing_export.csv.gpg --expires-in 86400
# Step 5: Send secure link + decryption password via separate channel
```

6. Monitoring and Compliance:

- Set up DataDog alert for any access to marketing_approved_students view
- Schedule automatic view deletion after campaign end date
- Require Marketing to provide deletion certificate after 30 days
- Audit log review in weekly DevOps security meeting

Required Consultations Before Final Approval

Who Else Must Approve This Request:

1. Data Protection Officer (DPO) / Legal Counsel:

- Verify marketing consent percentage and validity
- Review Data Processing Agreement language
- Confirm Ghana DPA compliance
- Approve purpose change from education to marketing

2. Chief Information Security Officer (CISO):

- Review security controls and encryption methods
- Approve temporary IAM role creation
- Sign off on data handling procedures
- Assess risk of 34,000 record export

3. Head of Student Services:

- Confirm appropriateness of marketing campaign timing
- Review student experience impact
- Approve use of educational platform for marketing

4. Engineering Manager:

- Review technical implementation plan
- Allocate DevOps resources for secure export process
- Approve database view creation and access patterns

Action Steps - Implementation Timeline

Day	Action	Owner	Status
Monday PM	Obtain DPO/Legal approval Obtain CISO approval	DevOps (me)	PENDING

Tuesday AM	Sarah signs Data Processing Agreement Create database view and IAM role	Legal DevOps	PENDING
Tuesday PM	Generate encrypted export Provide secure download link	DevOps	PENDING
Wed-Fri	Marketing team uses data for campaign	Marketing	PENDING
Following Mon	Revoke Sarah's access Request deletion certificate	DevOps Compliance	PENDING

REQUEST 2: ANALYTICS PARTNERSHIP - AWS DATABASE ACCESS

Field	Details
Requestor	David Mensah, Head of Product
Department	Product Management
Request Date	Monday, February 9, 2026
Third Party	DataInsights Inc. (US-based analytics firm)
Data Requested	AWS database access for student learning pattern analysis
Access Method	Direct database login credentials (attached to ticket!)
Data Involved	Student activity logs (INTERNAL) + Student profiles (CONFIDENTIAL)
Compliance Note	Subject to Ghana Data Protection Act (2012)

■ CRITICAL SECURITY ALERT ■

Database credentials were attached to the support ticket in PLAIN TEXT. This represents an immediate security incident. Actions taken:
1. Credentials immediately rotated (Monday 10:15 AM)
2. Incident logged in security incident management system (INC-2026-0147)
3. Security awareness training scheduled for David Mensah
4. Ticket moved to encrypted incident response platform

OFFICIAL DECISION FORM - REQUEST #2

DECISION	**DENY (with alternative solution offered)**
Lifecycle Stage	**SHARE (Cross-border data transfer to third-party processor)**
Risk Assessment	**CRITICAL - Multiple severe violations and legal non-compliance**
Compliance Status	**VIOLATES Ghana DPA, GDPR equivalence, and data sovereignty laws**

Justification for DENIAL (DevOps Security Perspective)

Why This Request Must Be DENIED:

1. CRITICAL: Direct Database Access Violates Infrastructure Security:
Providing database login credentials to a third party would:
- Grant unrestricted access to ALL tables (not just student data)
- Expose database schema and business logic to external party

- Create unmonitored access vector (no audit trail of queries executed)
- Violate AWS Well-Architected Framework security pillar
- Enable potential data exfiltration of entire 50,000+ student database
- Bypass all application-layer access controls and validation
- Give write access (potential for data corruption or deletion)

From a DevOps perspective, this is equivalent to giving a third party root access to production servers. ABSOLUTELY UNACCEPTABLE under any circumstances.

2. Legal Compliance Red Flags - Ghana Data Protection Act Violations:

a) Cross-Border Data Transfer Without Adequate Safeguards:
Ghana DPA Section 37 requires that data transferred outside Ghana must be to countries with "adequate level of protection." The United States does NOT have blanket adequacy determination from Ghana's Data Protection Commission.

Required for lawful transfer:
- Standard Contractual Clauses (SCCs) approved by Data Protection Commission
- Data Processing Agreement meeting Ghana DPA requirements
- Technical safeguards (encryption, access controls)
- Legal review and DPO approval
- Student notification of international transfer

NONE of these are in place. This transfer would be ILLEGAL.

b) Third-Party Processor Requirements:
Ghana DPA requires data controllers (us) to:
- Conduct due diligence on processors (DataInsights Inc.)
- Verify processor's data protection capabilities
- Enter formal data processing agreement
- Ensure processor doesn't use data for own purposes
- Maintain ability to audit processor's handling

David has "signed a partnership" but provided NO documentation of:
- DataInsights Inc.'s data protection certification
- Background on their security practices
- Insurance or liability coverage
- Subprocessor list (who else might access our data)
- Data retention and deletion commitments

c) Purpose Limitation Violation:
Student data was collected for "educational services." Using it for third-party analytics research requires either:
- Explicit student consent for this new purpose, OR
- Legitimate interest assessment with privacy impact analysis

Neither exists. Students enrolled expecting their data to stay within EduConnect's educational platform, not be shipped to US analytics firms.

3. Principle of Least Privilege - Grossly Violated:
Even IF legal compliance were addressed, direct database access violates least privilege:
- DataInsights needs AGGREGATED, ANONYMIZED analytics data
- They DON'T need: student names, emails, phone numbers, payment info
- They DON'T need: real-time database access
- They DON'T need: ability to run arbitrary SQL queries

Proper approach: Provide API endpoint with anonymized aggregate metrics, or export anonymized dataset.

4. Data Lifecycle Stage Risk - SHARE Without Controls:
This represents transition from STORE (in our secured AWS environment) to SHARE (with third-party processor). At this lifecycle stage, we must implement:

- Data minimization (remove unnecessary fields)
- Anonymization or pseudonymization
- Encryption in transit and at rest
- Access logging and monitoring
- Data retention agreements
- Right to audit

Direct database access provides NONE of these controls.

5. Infrastructure Risk - Potential Database Compromise:
From DevOps perspective, the risks include:

- **Credential Leakage:** If DataInsights is breached, our database credentials are exposed
- **Resource Exhaustion:** Poorly optimized analytics queries could crash production database
- **Data Corruption:** Accidental UPDATE/DELETE queries could corrupt student records
- **IP Exposure:** Database schema reveals our competitive advantage and business logic
- **Compliance Violation:** PCI-DSS non-compliance if payment data accessed
- **Monitoring Blind Spot:** No visibility into what queries they run or data they extract

6. Partnership Agreement Review - Missing Critical Elements:
David claims "partnership signed" but DevOps/Legal/Security were NOT involved. Red flags:

- No technical integration plan reviewed
- No security assessment of DataInsights Inc.
- No SLA for data protection
- No breach notification requirements
- No liability terms if student data is compromised
- No exit plan for ending partnership

This appears to be a business deal signed without technical or legal review.

ALTERNATIVE SOLUTION - Safe Analytics Partnership

DevOps-Recommended Approach to Enable Analytics Partnership Legally:

Phase 1: Legal and Compliance Foundation (Week 1-2)

1. **Due Diligence on DataInsights Inc.:**
- Request SOC 2 Type II certification
- Request ISO 27001 certification
- Conduct security questionnaire
- Review their data breach history
- Verify U.S. Privacy Shield or equivalent framework

2. **Legal Agreements:**
- Draft Data Processing Agreement (DPA) meeting Ghana DPA requirements
- Include Standard Contractual Clauses for international transfer
- Define data retention period (max 90 days post-project)
- Require deletion certificate upon completion
- Include right-to-audit clauses

3. **Student Consent/Notification:**
- Update Privacy Policy to disclose third-party analytics
- Email notification to all students about data processing
- Provide opt-out mechanism (students can exclude their data)
- Wait 30 days for opt-outs before proceeding

Phase 2: Technical Implementation (Week 3-4)

1. **Data Anonymization Pipeline:**

```
# Create anonymized analytics dataset
CREATE TABLE analytics_export AS
SELECT
SHA256(student_id) as anonymous_id, -- One-way hash, can't reverse
DATE_TRUNC('month', enrollment_date) as enrollment_month,
course_category,
completion_status,
AVG(quiz_score) as avg_score,
COUNT(login_events) as login_count,
-- NO names, emails, phone numbers, or precise dates
FROM students s
JOIN student_activity a ON s.id = a.student_id
WHERE s.opt_out_analytics = FALSE
GROUP BY anonymous_id, enrollment_month, course_category, completion_status;
```

2. **Secure Data Transfer Method:**
- NO direct database access
- Export anonymized dataset to encrypted S3 bucket
- Grant DataInsights read-only S3 access via IAM role
- Enable S3 access logging (who accessed what, when)
- Set bucket lifecycle policy to auto-delete after 90 days

3. **API Alternative (Preferred):**

Build REST API endpoint for analytics queries:

```
GET /api/v1/analytics/cohort-performance?course=python101&month;=2025-10
Response: { "avg_completion_rate": 0.78, "avg_score": 84.3, "total_students": 450 }
```

Benefits:
- Rate limiting (prevent data scraping)
- Query logging (audit trail)
- Access control (API key with expiration)

- Data validation (prevent injection attacks)
- Granular permissions (only aggregated data)

Phase 3: Monitoring and Compliance (Ongoing)

1. **Access Monitoring:**

- CloudWatch alarms for S3 bucket access
- Weekly access log review
- Anomaly detection for unusual query patterns

2. **Quarterly Audits:**

- Request proof of data deletion after 90 days
- Review DataInsights security posture
- Verify compliance with DPA terms

3. **Incident Response Plan:**

- If DataInsights is breached, revoke access immediately
- Notify students within 72 hours per Ghana DPA
- Document incident for Data Protection Commission

Timeline for Safe Implementation:

- Legal review and agreements: 2-3 weeks
- Student notification and opt-out period: 30 days
- Technical implementation: 1-2 weeks
- Security testing: 1 week
- **TOTAL: 8-10 weeks minimum**

If David's business need is urgent, we can provide anonymized sample dataset (1,000 students) immediately while full process is underway.

Required Documentation Before ANY Data Sharing

Documents that MUST be in place:

■ Data Processing Agreement (DPA) signed by DataInsights Inc. CEO
■ Standard Contractual Clauses for international transfer
■ DataInsights Inc. SOC 2 Type II report (not older than 12 months)
■ Data Protection Impact Assessment (DPIA) completed by DPO
■ Student privacy notice update approved by Legal
■ Security assessment of DataInsights by InfoSec team
■ Technical integration plan approved by Engineering Manager
■ Data retention and deletion schedule agreed upon
■ Incident response plan including DataInsights contact points
■ Approval from Data Protection Commission (if required for cross-border transfer)

Immediate Action Steps

Priority	Action	Owner	Deadline
P0 - URGENT	Notify David of DENIAL decision Explain legal/security issues	DevOps (me)	Monday 2PM
P0 - URGENT	Rotate database credentials that were exposed	DevOps	COMPLETED
P1 - High	Schedule meeting: Product, Legal, DevOps, DPO to discuss safe alternative	Product Manager	Tuesday AM

P1 - High	Initiate due diligence on DataInsights Inc.	Legal/InfoSec	This Week
P2 - Medium	Draft Data Processing Agreement template	Legal	Week 2
P2 - Medium	Build anonymized analytics dataset POC	DevOps/Data Eng	Week 2-3

REQUEST 3: RIGHT TO BE FORGOTTEN - ACCOUNT DELETION

Field	Details
Requestor	Comfort Asante, Customer Support Lead
Department	Customer Support
Request Date	Monday, February 9, 2026
Student	James Boateng (Student ID: STU-2025-04721)
Legal Basis	Right to be forgotten (Ghana DPA Section 32)
Account Status	Inactive - Last course completed 6 months ago (August 2025)
Outstanding Obligations	None - No pending payments or active enrollments
Data Classification	All student data classified as CONFIDENTIAL

OFFICIAL DECISION FORM - REQUEST #3

DECISION	**APPROVE (with partial data retention for legal compliance)**
Lifecycle Stage	**DESTROY (with legally-mandated ARCHIVE exceptions)**
Risk Assessment	**MEDIUM - Must balance right to erasure vs. legal retention requirements**
Compliance Status	**Ghana DPA Section 32 applies - Right to erasure with legal exemptions**

Legal Obligations Under Ghana Data Protection Act

Can This Request Be Fulfilled? YES - With Important Limitations

Ghana Data Protection Act Section 32 - Right to Erasure:
Data subjects have the right to obtain erasure of personal data where:
(a) The data is no longer necessary for the purpose collected
(b) The data subject withdraws consent
(c) The data subject objects to processing
(d) The personal data has been unlawfully processed

James Boateng's request meets criteria (a) and (b): his educational journey is complete, and he's withdrawing consent for further data processing.

HOWEVER - Legal Exemptions to Right to Erasure:
Ghana DPA Section 32(2) states erasure does NOT apply where retention is necessary for:
(a) Compliance with legal obligations
(b) Exercise or defense of legal claims
(c) Archiving purposes in the public interest

What This Means for EduConnect:

1. Financial Records (7-Year Retention - Tax Law Requirement):
Ghana Revenue Authority requires businesses to retain financial records for 7 years. This includes:

- Payment transactions
- Invoices and receipts
- Tax-related documentation

We MUST retain James's payment history until August 2032 (7 years from last transaction).

2. Academic Records (Indefinite Retention - Legitimate Interest):
Educational institutions have legitimate interest in maintaining:

- Course completion certificates (James may request replacement certificate)
- Grades and transcripts (for employment verification)
- Academic integrity records (to prevent fraud)

However, we can ANONYMIZE these records (replace name with "Student STU-2025-04721").

3. Legal Claims (6-Year Retention - Statute of Limitations):
Ghana's Limitation Act requires potential legal claims be retained for 6 years. We must keep:

- Terms of Service acceptance logs
- Account activity logs (in case of dispute)

This data can be retained in anonymized form in our legal hold system.

Data Deletion vs. Retention Matrix

Data Category	Action	Justification	Timeline
Profile Info (name, email, phone, photo)	DELETE	No longer needed, no legal exception	Immediate (30 days)
Login Credentials (password hash, 2FA)	DELETE	Account closed, no access needed	Immediate
Course Activity Logs (videos watched, quizzes taken)	DELETE	Not required for legal compliance	Immediate (30 days)
Forum Posts & Comments	ANONYMIZE	Public educational resource for other students	30 days
Payment Transactions	RETAIN (anonymized)	Tax law 7-year requirement	Until Aug 2032
Course Completion Certificates	ANONYMIZE	May need to issue replacement	Indefinite
Final Grades & Transcripts	ANONYMIZE	Employment verification	Indefinite
Support Tickets	ANONYMIZE	Legal claims defense	6 years
Audit Logs (access, changes)	RETAIN (anonymized)	Security compliance	7 years

DevOps Technical Implementation - Data Lifecycle DESTROY Stage

Automated Deletion Process (DevOps Implementation):

Step 1: Verification and Validation (Day 1)

```
# Verify student identity and no pending obligations
SELECT student_id, account_status, outstanding_balance, active_courses
FROM students WHERE student_id = 'STU-2025-04721';

# Check: No active enrollments, zero balance
IF outstanding_balance = 0 AND active_courses = 0:
PROCEED with deletion
ELSE:
DENY request until obligations resolved
```

Step 2: Data Backup Before Deletion (Day 1)

```
# Create encrypted backup (recovery in case of error)
pg_dump -t students -t student_activity -t payments \
--where="student_id='STU-2025-04721'" \
| gpg --encrypt > /backups/deletion_backup_STU-2025-04721.sql.gpg

# Retention: 90 days, then auto-delete
```

Step 3: Execute Multi-Table Deletion (Days 2-30)

```
-- Transaction ensures atomicity (all or nothing)
BEGIN TRANSACTION;

-- Delete from least to most critical tables
DELETE FROM session_logs WHERE student_id = 'STU-2025-04721';
DELETE FROM course_activity WHERE student_id = 'STU-2025-04721';
DELETE FROM quiz_attempts WHERE student_id = 'STU-2025-04721';
DELETE FROM video_progress WHERE student_id = 'STU-2025-04721';
DELETE FROM notifications WHERE student_id = 'STU-2025-04721';
DELETE FROM student_preferences WHERE student_id = 'STU-2025-04721';

-- Anonymize (not delete) legally-required data
UPDATE payments SET
student_name = 'DELETED USER',
student_email = 'deleted@educonnect.gh',
student_phone = NULL
WHERE student_id = 'STU-2025-04721';

UPDATE course_completions SET
student_name = 'Student STU-2025-04721'
WHERE student_id = 'STU-2025-04721';

UPDATE support_tickets SET
requester_name = 'ANONYMIZED',
requester_email = 'anonymized@educonnect.gh'
WHERE student_id = 'STU-2025-04721';

-- Finally, anonymize main student record
UPDATE students SET
first_name = 'DELETED',
last_name = 'USER',
email = 'deleted_' || student_id || '@educonnect.gh',
phone = NULL,
date_of_birth = NULL,
address = NULL,
photo_url = NULL,
password_hash = NULL,
account_status = 'DELETED',
deletion_date = CURRENT_TIMESTAMP,
deletion_reason = 'User requested - Right to be forgotten'
WHERE student_id = 'STU-2025-04721';

COMMIT TRANSACTION;
```

Step 4: Delete from External Systems (Days 2-30)

- Remove from email marketing platform (Mailchimp/SendGrid)
- Delete from customer support system (Zendesk/Intercom)
- Remove from analytics platforms (Google Analytics, Mixpanel)
- Delete from CDN cached files (profile photos)
- Remove from backup systems (except legal-hold backups)

Step 5: Third-Party Notification (Day 30)

Notify any third-party processors (if data was shared):

- Cloud storage providers (AWS S3, CloudFlare)
- Payment processors (Stripe, Paystack)
- Communication platforms (Twilio for SMS)

Request deletion confirmation from each processor.

Step 6: Deletion Certificate (Day 30)

Generate automated deletion certificate to send to James Boateng:

```
DELETION CERTIFICATE
Student: James Boateng (STU-2025-04721)
Request Date: February 9, 2026
Completion Date: March 11, 2026

Data Deleted:
- Personal information (name, email, phone, address, photo)
- Login credentials
- Course activity logs (154 records)
- Video progress (89 courses)
- Quiz attempts (234 quizzes)
- Session logs (1,247 sessions)

Data Retained (Legally Required):
- Payment records (anonymized, retained until 2032 per tax law)
- Course certificates (anonymized, indefinite retention)
- Support tickets (anonymized, retained 6 years)

Verified by: DevOps Automation System
Contact: privacy@educonnect.gh for questions
```

Customer Support Standard Operating Procedure

What Process Should Customer Support Follow? (For Comfort Asante)

Standard Operating Procedure: Right to Erasure Requests

Phase 1: Request Reception and Validation (Day 1)
1. **Verify Student Identity:**
• Ask for account email verification (send code to registered email)
• Request last 4 digits of payment method used
• Verify date of birth or student ID number
• PURPOSE: Prevent fraudulent deletion requests

2. **Check Account Status:**
• Outstanding balance? → Must be resolved before deletion
• Active course enrollments? → Notify student of loss of access
• Pending certificates? → Offer to send before deletion
• Refund eligibility? → Process before deletion

3. **Inform Student of Implications:**
Send standard email template:
"Your deletion request will result in:
• *Loss of access to all courses and materials*
• *Deletion of certificates (download before deletion)*
• *Inability to recover account (permanent action)*
• *Some anonymized data retained for legal compliance*

To proceed, reply 'CONFIRM DELETE' within 7 days."

Phase 2: Confirmation and Grace Period (Days 2-7)
1. Wait for explicit written confirmation
2. 7-day grace period (allow student to change mind)
3. During grace period: Account suspended but not deleted

Phase 3: Escalation to DevOps (Day 8)
1. **Create Deletion Ticket:**
• Ticket System: JIRA or ServiceNow
• Priority: P2 (process within 30 days)
• Include: Student ID, confirmation email, verification logs

2. **Assign to DevOps Team:**
DevOps runs automated deletion script (see technical implementation above)

Phase 4: Follow-Up (Day 30)
1. DevOps provides deletion certificate
2. Customer Support sends certificate to student
3. Mark ticket as RESOLVED
4. Log completion in compliance register

Important Notes for Customer Support:
• NEVER manually delete database records (risk of incomplete deletion)
• ALWAYS use official deletion request form
• DOCUMENT all steps in ticket (audit trail)
• If student is under 18: Require parent/guardian consent
• If student has ongoing legal matter: Escalate to Legal before proceeding
• If deletion would harm others: Escalate to DPO (e.g., group project data)

Action Steps - James Boateng Deletion Request

Day	Action	Owner	Status
Day 1 (Today)	Verify James Boateng identity Send implications email Request confirmation	Customer Support	PENDING
Day 2-7	7-day grace period Account suspended, not deleted Wait for CONFIRM DELETE reply	Customer Support	PENDING
Day 8	Create deletion ticket in JIRA Assign to DevOps team Provide verification docs	Customer Support	PENDING
Day 8-30	Execute automated deletion script Delete from external systems Notify third-party processors	DevOps	PENDING
Day 30	Generate deletion certificate Send to James Boateng Mark ticket RESOLVED	DevOps + Support	PENDING

CONCLUSION - KEY TAKEAWAYS FOR DEVOPS

Summary of Three Data Access Decisions:

Request 1 - Marketing Campaign: CONDITIONAL APPROVAL
Approved with significant safeguards because:
- Data minimization reduces exposure from 50K to 34K consented students
- Secure transfer mechanisms (SFTP, encryption) protect data in transit
- Time-limited access with automatic revocation prevents indefinite exposure
- Data Processing Agreement creates legal accountability

DevOps Role: Build secure export pipeline, create read-only database views, implement monitoring.

Request 2 - Analytics Partnership: DENY
Denied because:
- Direct database access is unacceptable security practice (violates least privilege)
- Cross-border transfer to US without adequate safeguards violates Ghana DPA
- No due diligence on third-party processor
- Missing required legal agreements (DPA, SCCs)
- Students not notified of international data processing

DevOps Role: Rotate compromised credentials, propose safe alternative (API or anonymized export), build technical controls for future partnerships.

Request 3 - Account Deletion: APPROVE (with partial retention)
Approved with legal exemptions because:
- Right to erasure under Ghana DPA applies
- No outstanding student obligations
- Financial and legal records must be retained per tax/statute law
- Academic records can be anonymized instead of deleted

DevOps Role: Execute multi-table deletion script, coordinate with external systems, generate deletion certificate, document for compliance audit.

Common Themes - DevOps Data Governance Principles:

1. Principle of Least Privilege:
- Grant minimum necessary access, not "full database"
- Use read-only access, views, and APIs instead of direct credentials
- Time-limit all elevated permissions

2. Data Lifecycle Management:
- Understand which lifecycle stage applies (Use, Share, Store, Destroy)
- Apply appropriate controls at each stage
- Document retention requirements vs. deletion obligations

3. Compliance-First Mindset:
- Ghana Data Protection Act is law, not suggestion
- Cross-border transfers require legal frameworks
- Right to erasure has legal exemptions (tax, statute of limitations)
- Consult DPO/Legal before granting CONFIDENTIAL data access

4. Security by Design:
- Never share database credentials with third parties
- Encrypt data in transit and at rest

- Implement audit logging for all data access
- Use automated processes for deletion (prevents human error)

5. Documentation and Audit Trail:

- Every decision must be documented with justification
- Maintain logs of who accessed what data when
- Create certificates for deletions and transfers
- Prepare for regulatory audits and legal discovery

DevOps's Role in Data Governance:

As DevOps engineers, we are the last line of defense against data breaches and compliance violations. We must:

- Question requests that seem to violate security best practices
- Propose technical alternatives that meet business needs safely
- Implement infrastructure controls that enforce policies automatically
- Monitor and audit data access patterns
- Educate colleagues on data classification and lifecycle

These three requests demonstrate that saying "yes" requires careful analysis, legal consultation, and technical safeguards. Sometimes the most responsible answer is "no, but here's a better way."

Next Steps for EduConnect:

1. Formalize data access request process (standardized forms and approval workflows)
2. Implement automated data classification tagging in database
3. Build self-service anonymization tools for internal teams
4. Create data access review board (Legal, InfoSec, DevOps, DPO)
5. Quarterly audit of all third-party data processors
6. Annual Ghana DPA compliance training for all staff

Report prepared by: DevOps Engineering Team
Contact: devops@educonnect.gh | security@educonnect.gh

Required Approvals:

■ Chief Information Security Officer (CISO)
■ Data Protection Officer (DPO)
■ Head of Legal & Compliance
■ Chief Technology Officer (CTO)