DIVERGENT LEARNING COMMUNITY CIC

Educational Document Redaction and Cognitive Profiling Process

Policy and Procedure Document

Document Version: Version 3.0

Effective Date: February 2026 (updated 18 November 2026)

Review Date: November 2027

Responsible Person: Claudia Celi, Founder

Document Status: Active

1. PURPOSE AND SCOPE

1.1 Purpose

This policy establishes the procedures for securely handling, redacting, and processing educational documents submitted by parents/guardians for the purpose of creating cognitive profiles for learners aged **7-16** at Divergent Learning Community.

1.2 Scope

This policy applies to:

- All community members handling children's documentation
- All educational reports, assessments, and records submitted by parents/guardians
- The redaction and cognitive profiling process
- Storage, retention, and destruction of both original and redacted documents

1.3 Legal and Regulatory Framework

This policy ensures compliance with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Children and the UK GDPR (ICO Guidance)
- Keeping Children Safe in Education (KCSIE) (latest statutory guidance)

- UN Convention on the Rights of the Child

2. DEFINITIONS

Personal Data: Any information relating to an identified or identifiable child, including names, dates of birth, addresses, NHS numbers, school names, and any other identifying information.

Special Category Data: Sensitive personal data requiring higher protection, including health information, information about cognitive profiles, and any data relating to a child's physical or mental health.

Redaction: The process of permanently removing or obscuring personal and sensitive information from documents to protect privacy whilst retaining educationally relevant content.

Cognitive Profile: A comprehensive assessment of a learner's strengths across the MIND Strengths Framework (Material, Interconnected, Narrative, Dynamic reasoning), created from redacted educational documents.

Data Controller: Divergent Learning Community CIC, responsible for determining how and why personal data is processed.

Parent/Guardian: Person(s) with parental responsibility for the child as defined by UK law.

3. ROLES AND RESPONSIBILITIES

3.1 Founder (Data Controller)

- Overall responsibility for data protection compliance
- Approval of redaction procedures and cognitive profiles
- Ensuring community member training on data protection and safeguarding
- Managing relationships with parents/guardians regarding data processing

3.2 Designated Data Handler

- Receiving and logging all incoming documents
- Carrying out redaction using DLC’s manual method and verifying redaction quality
- Maintaining secure storage systems

- Managing document retention and destruction schedules

3.3 Cognitive Profile Analyst (AI-assisted)

- Analysing redacted documents to create cognitive profiles
- Ensuring no identifiable data is used in profile creation
- Maintaining confidentiality of all information processed

4. UNDERSTANDING DLC'S CAPACITY

4.1 What DLC Can Support

DLC is designed to support children with diverse cognitive profiles through:

- Strengths-based, individualised learning approaches
- Different MIND reasoning types and processing speeds
- Small group collaborative work
- Each child's interests and strengths as starting points

4.2 What DLC Cannot Provide

As a small learning community, DLC **cannot** provide:

- Intensive 1:1 specialised behavioural intervention
- Clinical therapeutic or mental health support
- Specialized autism programmes (ABA, intensive sensory programmes)
- Medical management or crisis intervention beyond basic first aid
- Full-time care for severe anxiety, self-regulation challenges, or complex trauma

4.3 Document Processing and Capacity Assessment

When processing educational documents, the Cognitive Profile Analyst will assess whether the child's profile suggests support needs beyond DLC's capacity. If this is identified:

- Parents will be contacted to discuss concerns

- Alternative provisions may be recommended
- Placement may not be offered if needs exceed DLC's capacity
- This protects both the child and the community

This is about being honest that DLC works best when a child's support needs align with our current capacity and expertise.

5. SAFEGUARDING CHILDREN'S DATA

5.1 Core Safeguarding Principles

DLC recognises that children (defined as anyone under 18 years of age) are entitled to enhanced protection of their personal data under UK GDPR and Data Protection Act 2018.

Special Protections for Children:

- All children's data is processed with additional security measures
- Information is processed only for the explicit purpose of educational support
- Age-appropriate communication when directly engaging with learners
- Enhanced security protocols for special category data relating to children's health and learning profiles

5.2 Parental Consent Requirements

- **Children under 13:** Parental consent is required for all data processing
- **Children aged 13-16:** Parental consent is required given the nature of educational support services
- Clear, age-appropriate privacy information provided to both parents and children
- Parents maintain the right to withdraw consent at any time

5.3 Safeguarding Data Sharing

Whilst DLC does not generally share children's data with third parties, this policy acknowledges:

- The lawful basis to share information without consent where necessary to protect a child from harm

- Compliance with "Safeguarding of children and individuals at risk" provisions in Data Protection Act 2018
- Requirement to report any safeguarding concerns to appropriate authorities regardless of data protection considerations
- **If any document reveals safeguarding concerns, DLC will follow statutory safeguarding procedures and may share information with relevant authorities without parental consent where necessary to protect the child**

5.4 Rights of the Child

Children and their parents have the following rights:

- **Right of Access:** Request to see what data is held
- **Right to Rectification:** Request correction of inaccurate data
- **Right to Erasure:** Request deletion of data (subject to legitimate retention requirements)
- **Right to Restriction:** Request limitation on how data is used
- **Right to Data Portability:** Receive data in a structured, commonly used format
- **Right to Object:** Object to certain types of processing

Requests must be responded to within 30 days.

6. DATA RECEIPT AND CONSENT PROTOCOL

6.1 Initial Parent/Guardian Contact

Before any documents are submitted, parents/guardians must:

1. Receive Information Pack containing:

- Privacy Notice explaining how data will be processed
- Clear explanation of the redaction process
- Description of how cognitive profiles are created
- Information about DLC's capacity and limitations
- Information about data storage, retention, and destruction
- Explanation of parental and child rights under UK GDPR

- Contact details for queries or concerns

2. Provide Informed Consent via signed consent form including:

- Permission to process their child's educational documents
- Understanding that original documents will be redacted
- Agreement to the purpose of cognitive profiling
- Understanding of DLC's capacity limitations
- Confirmation of their right to withdraw consent
- Understanding of data retention periods
- Acknowledgement that original documents will be securely destroyed after processing

3. Verify Parental Responsibility:

- Confirm legal authority to provide consent
- Request proof of parental responsibility if unclear

6.2 Document Submission Methods

Accepted Submission Methods:

- Secure email to designated DLC address (encrypted if possible)
- Hand delivery to DLC premises with signed receipt
- Secure file transfer portal (if implemented)

Accepted Document Formats:

- PDF documents
- Microsoft Word documents (.doc, .docx)
- Scanned images (JPEG, PNG)
- Official educational reports in original format

Document Receipt Log:

All received documents must be logged immediately with:

- Date and time of receipt
- Child's name (temporary identifier only)
- Parent/guardian name
- Document type and source (e.g., "Educational Psychology Report, 2024")
- Method of receipt
- Community member receiving document
- Unique reference number assigned

7. REDACTION PROCEDURE

7.1 Redaction Method

DLC uses a text-based manual redaction method rather than redaction software. Only the relevant sections of a document are copied into a fresh working document, every identifier is removed using the checklist in section 7.2, and a second check (by a second trained community member where available, otherwise a separate, unhurried read-through on a different day) is completed before any text is used. Black-box redaction on top of PDFs is never used, because hidden text can often be recovered. Scanned or handwritten reports are retyped, leaving out identifying details. Dedicated redaction software may be reconsidered if DLC grows; any change requires review against this policy and approval by the Founder.

7.2 Information to be Redacted

Mandatory Redactions:

- Full names (child, family members, teachers, professionals)
- Dates of birth and exact ages (replace with an age band if needed, e.g. "aged 7–9")
- Addresses (home, school, any location)
- Postcodes
- NHS numbers or patient identification numbers
- School names (replace with "mainstream school" or "primary school")
- Email addresses

- Telephone numbers
- National Insurance numbers (if present)
- Case numbers or reference numbers
- Photographs or images
- Signatures
- Ethnicity identifiers (unless specifically relevant to learning profile)
- Religious information (unless specifically relevant)

Information to be Retained (Non-Identifying):

- Age band of child (e.g. 7–9)
- Key stage (where educationally relevant)
- Gender (if relevant to assessment)
- Information about cognitive profile (e.g., "autism", "ADHD", "dyslexia")
- Assessment scores and data (e.g., IQ scores, reading ages)
- Cognitive strengths and challenges described
- Recommendations for educational support
- Therapy or intervention history (anonymised)
- Academic performance data
- Behavioural observations

7.3 Redaction Process Steps

Step 1: Secure Environment Setup

- Work on dedicated, password-protected computer
- Ensure screen privacy (no visibility to unauthorised persons)
- Disable auto-save to cloud services
- Close unnecessary applications

Step 2: Document Preparation

- Create working folder with unique reference number
- Copy original document to working folder
- Log start of redaction process with date/time

Step 3: Create the Working Text

- Copy only the educationally relevant sections into a fresh working document (retype scanned or handwritten text)
- Use find-and-replace and a careful search for:
- Common UK names (if known from consent form)
- Date formats (DD/MM/YYYY)
- Postcode patterns
- NHS number formats
- Email formats
- Phone number formats
- Remove or replace every match (for example, "the child", "a professional")
- Record which checklist items were completed

Step 4: Manual Review

- Carefully read entire document
- Identify any information missed by the search
- Look for:
- Names in unusual contexts or spellings
- Addresses described rather than formatted
- Identifying details in narrative text
- Headers, footers, and metadata
- Embedded objects or images

- Delete identified content from the working text

Step 5: Quality Verification

- Second check of the entire working text (by a second trained community member where available, otherwise a separate read-through on a different day)
- Confirm all personal identifiers removed
- Verify educational content remains intact and comprehensible
- Confirm the working text was created fresh, so it carries no metadata from the original
- Confirm no identifying text remains anywhere in the working text

Step 6: Export and Verification

- Save the redacted working text as a new document
- Search the saved text once more for names, dates, places and numbers
- Confirm the original document is not attached to or embedded in the redacted text
- Save to secure "Redacted Documents" folder with reference number

Step 7: Documentation

- Update processing log:
- Date/time redaction completed
- Community member who performed redaction
- Redaction checklist completed and second check recorded
- Any issues or notes
- Quality verification confirmation

7.4 Quality Assurance

Dual Verification System:

- Every redaction receives a second check before any text is used
- Periodic review of completed checklists by the Founder

- Any quality issues trigger immediate review of all recent redactions

Common Error Prevention:

- Checklist system for each redaction
- Regular training refreshers
- Updating the checklist whenever a gap is found
- Learning from any identified mistakes

8. SECURE STORAGE

8.1 Original Documents

Storage Location:

- Physical storage: Locked filing cabinet in secure office
- Digital storage: Encrypted folder on password-protected computer (not cloud-based initially)

Access Control:

- Only authorised Data Handler has access
- Access log maintained for all retrievals
- Physical keys held by two designated community members

Retention Period:

- Original documents retained for 30 days after redaction completion
- Allows time for verification and any parent queries
- After 30 days: Secure destruction (see Section 10)

8.2 Redacted Documents

Storage Location:

- Encrypted folder on secure computer
- Separate from originals

- Regular backups to encrypted external drive stored securely

Naming Convention:

- DLC_[Reference Number]_[Document Type]_Redacted_[Date]
- Example: DLC_2026001_EdPsychReport_Redacted_20260224

Access Control:

- Data Handler (processing)
- Cognitive Profile Analyst (analysis only)
- Founder (quality oversight)

Retention Period:

- Securely destroyed within 30 days of profile completion
- Only the strengths profile is kept after this point
- Earlier destruction on request or if consent is withdrawn (within 72 hours)

8.3 Cognitive Profiles

Storage Location:

- Separate encrypted database or folder
- Completely isolated from original/redacted documents
- No cross-references to original document source

Content:

- MIND Strengths assessment results
- Interests and engagement
- Recommended learning approaches
- Historical profile updates (tracking development)
- No personal identifying information

Access Control:

- Learning facilitators requiring information for educational planning
- Parents/guardians (can request copy)
- Child (age-appropriate access from age 13+)

Retention Period:

- Retained whilst child is at DLC
- Retained for 2 years after child leaves DLC (to support transitions)
- Destroyed after retention period unless parent requests transfer to new provider

9. ANALYSIS AND COGNITIVE PROFILING PROCESS

9.1 AI-Assisted Analysis Protocol

Process:

1. **Redacted text entered into Claude (Anthropic) in an incognito chat, with model training switched off on DLC's account; feedback buttons are never used**

2. **AI analyses content for:**

- Evidence of Material reasoning (spatial, mechanical, hands-on learning)
- Evidence of Interconnected reasoning (systems thinking, patterns, relationships)
- Evidence of Narrative reasoning (storytelling, sequential, contextual)
- Evidence of Dynamic reasoning (experimentation, movement, kinaesthetic)
- Interests, contexts and access supports that help the child engage

3. **AI generates draft cognitive profile with:**

- Dominant reasoning strengths
- Supporting strengths and interests
- Recommended learning environments
- Suggested teaching approaches

- Potential challenge areas and support strategies

4. **Human review and refinement:**

- Learning facilitator reviews AI-generated profile
- Validates conclusions against original redacted documents
- Adds professional insights and context
- Ensures profile is constructive and strengths-focused

5. **Capacity assessment:**

- Profile reviewed to identify if child's needs exceed DLC's capacity
- If concerns identified, discussion with parents before placement decision

6. **Quality assurance:**

- Profile reviewed for any identifying information (should be none)
- Profile checked for accuracy and usefulness
- Profile formatted for parent/learning facilitator use

9.2 No Re-Identification

Critical Safeguards:

- Cognitive profiles contain NO names, dates, or locations
- Profiles are labelled only with reference numbers
- Separate cross-reference document (stored securely) links reference numbers to child identity
- Cross-reference document accessible only to Data Controller
- Only redacted text is ever entered into AI systems; incognito chats are not saved to the chat history

9.3 Parent Communication

Profile Delivery:

- Completed cognitive profile sent to parent/guardian within 21 days of document submission
- Accompanied by explanatory guidance on interpreting and using the profile
- Clear communication about whether DLC can appropriately support the child's needs
- Offer of consultation to discuss findings and recommendations
- Clear statement of strengths-based approach and celebration of cognitive diversity

Parent Rights:

- Request modifications to profile if inaccuracies identified
- Request deletion of profile at any time
- Request transfer of profile to other educational providers

10. DATA DESTRUCTION PROCEDURES

10.1 Original Documents (After 30-Day Retention)

Physical Documents:

- Cross-cut shredding (minimum P-4 security level)
- Shredding witnessed and logged
- Shredded material disposed of securely
- Certificate of destruction retained

Digital Documents:

- Secure deletion using file wiping software (minimum 3-pass overwrite)
- Confirmation of deletion logged

- Regular verification that documents are irrecoverable
- Backup copies also securely wiped

10.2 Redacted Documents (At End of Retention Period)

Trigger Events:

- 30 days after profile completion
- Parent/guardian requests deletion
- DLC closes operations (all data securely destroyed)

Process:

- Secure deletion as per original documents
- Confirmation sent to parent/guardian if deletion was requested
- Destruction log maintained

10.3 Cognitive Profiles

Trigger Events:

- 2 years after child leaves DLC (unless transferred)
- Parent/guardian requests deletion
- DLC closes operations

Process:

- Secure deletion from all systems
- Confirmation to parent/guardian
- Cross-reference entry deleted
- Destruction logged

10.4 Destruction Logs

Maintained Records:

- Date of destruction
- Type of data destroyed
- Reference numbers
- Method of destruction
- Community member responsible
- Witness (for physical destruction)

Retention of Logs:

- Destruction logs retained for 7 years
- Provides audit trail for compliance demonstration

11. DATA BREACH PROCEDURES

11.1 Definition of Data Breach

A data breach includes:

- Unauthorised access to personal data
- Accidental disclosure to wrong recipient
- Loss or theft of devices containing data
- Ransomware or hacking attacks
- Physical document misplacement
- Unintended sharing of identifiable information

11.2 Immediate Actions (Within 1 Hour)

1. Containment:

- Stop the breach if ongoing
- Secure systems and documents
- Isolate affected systems if digital breach

2. Assessment:

- Identify what data was affected
- Determine how many children are affected
- Assess risk of harm to children

3. Notification:

- Inform Data Controller (Founder) immediately
- Document all known details

11.3 Reporting to ICO (Within 72 Hours)

If breach meets notification criteria:

- Report to Information Commissioner's Office (ICO) within 72 hours of discovery
- Include:
- Nature of the breach
- Categories and approximate number of children affected
- Categories and approximate number of records affected
- Contact details for further information
- Description of likely consequences
- Measures taken or proposed to address the breach

Notification Criteria:

- Risk to children's rights and freedoms
- Potential for identity theft, discrimination, or reputational damage
- Loss of confidentiality of special category data
- Any unauthorised access to safeguarding information

11.4 Notification to Affected Families

When Required:

- High risk to children's rights and freedoms

- Potential for significant harm

Communication Method:

- Direct contact with affected parents/guardians
- Clear, non-technical language
- Explain:
- What happened
- What data was affected
- What we are doing
- What they should do (if anything)
- How to contact us for questions
- Right to complain to ICO

11.5 Prevention and Learning

Post-Breach Actions:

- Full investigation to determine cause
- Document lessons learned
- Update procedures to prevent recurrence
- Community member retraining if needed
- Consider if additional security measures required

12. COMMUNITY MEMBER TRAINING AND COMPETENCY

12.1 Mandatory Training

All community members handling children's data must complete:

1. UK GDPR and Data Protection Fundamentals

- Understanding of GDPR principles
- Rights of children under GDPR

- Specific requirements for educational data
- Consequences of non-compliance

2. Safeguarding Children's Data

- Enhanced protections for children under 18
- Recognising safeguarding concerns in documents
- When to share data without consent
- Working with Keeping Children Safe in Education guidelines

3. Redaction Method Training

- Practical training on DLC’s manual redaction method and checklist
- Understanding why black-box PDF redaction is not used
- Quality verification procedures
- Common errors and how to avoid them

4. Data Breach Recognition and Response

- Identifying potential breaches
- Immediate response protocols
- Reporting requirements
- Prevention strategies

12.2 Competency Assessment

Initial Competency:

- Written test on GDPR and safeguarding requirements (80% pass)
- Supervised redaction of 5 practice documents
- Independent redaction of 3 documents with quality verification

- Demonstration of breach response procedures

Ongoing Competency:

- Annual refresher training
- Quality audits of redaction work
- Updates when legislation or procedures change

12.3 Training Records

Documentation:

- Training dates and content
- Assessment results
- Certificates of completion
- Refresher training schedule

Retention:

- Held in community member files
- Reviewed during annual reviews
- Updated as role requirements change

13. MONITORING AND AUDIT

13.1 Regular Monitoring

Monthly Review:

- Number of documents processed
- Processing times
- Any quality issues identified
- Parent queries or concerns
- System security status

Quarterly Review:

- Sample audit of redacted documents (10% of quarter's volume)
- Review of access logs
- Storage security verification
- Backup integrity check

Annual Review:

- Full policy review and updates
- Community member competency assessments
- Redaction method and technology review
- Retention schedule verification
- Data breach prevention measures assessment

13.2 Audit Trail

Maintained Records:

- Document receipt logs
- Redaction processing logs
- Access logs for stored data
- Destruction logs
- Training records
- Incident and breach reports
- Quality assurance findings

Audit Trail Retention:

- 7 years minimum
- Demonstrates compliance to ICO if required
- Supports continuous improvement

13.3 Third-Party Audit

When Required:

- If processing more than 50 children's records per year
- If breach has occurred
- As good practice every 3 years
- If significant procedure changes implemented

Audit Scope:

- Review of compliance with this policy
- Testing of redaction quality
- Storage security assessment
- Community member competency verification
- Recommendations for improvement

14. PARENTAL ACCESS AND RIGHTS

14.1 Subject Access Requests (SARs)

Process:

1. Parent/guardian submits written request for access to data held about their child
2. Identity verification (to prevent unauthorised access)
3. Response within 30 days (extendable by 2 months if complex, with explanation)
4. Provide:

- Confirmation of data held
- Copy of redacted documents (if requested)
- Copy of cognitive profile
- Explanation of processing purposes

- Information about retention periods
- Details of any third-party recipients (if applicable)

No Fee:

- SARs are provided free of charge
- Fee may be charged only for manifestly unfounded or excessive requests

14.2 Right to Rectification

Process:

1. Parent identifies inaccurate information in cognitive profile
2. Request submitted in writing
3. Verification of inaccuracy
4. Correction made within 30 days
5. Confirmation sent to parent
6. If profile shared with others (e.g., learning facilitators), corrections distributed

14.3 Right to Erasure ("Right to be Forgotten")

Process:

1. Parent requests deletion of child's data
2. Assessment of legitimate grounds for retention
3. If no overriding legitimate interest:

- Immediate cessation of processing
- Deletion within 30 days
- Confirmation to parent

4. If legitimate grounds exist:

- Explanation to parent
- Right to complain to ICO explained

Legitimate Grounds to Retain:

- Legal obligation (limited for DLC)
- Public interest (not typically applicable)
- Safeguarding concerns requiring retention

14.4 Right to Restriction

Process:

1. Parent requests limitation on processing (e.g., "don't use for profile updates")
2. Assessment of request
3. Implementation of restriction
4. Note added to records
5. Confirmation to parent

14.5 Right to Data Portability

Process:

1. Parent requests transfer of data to another provider
2. Cognitive profile provided in structured, machine-readable format (JSON or CSV)
3. Direct transfer to new provider if technically feasible
4. Completion within 30 days
5. No fee charged

14.6 Right to Object

Process:

1. Parent objects to processing (e.g., use of AI for profiling)
2. Assessment of objection grounds
3. If compelling legitimate grounds cannot be demonstrated:
   - Processing stopped
   - Alternatives discussed
4. If legitimate grounds exist:
   - Explanation to parent

- Right to complain to ICO explained

15. COMPLAINTS AND ESCALATION

15.1 Internal Complaints

Process:

1. Complaint received in writing or verbally
2. Acknowledgement within 2 working days
3. Investigation assigned to community member (not involved in original processing)
4. Investigation completed within 14 days
5. Written response to complainant with findings and actions
6. If not satisfied, escalation to Founder/Data Controller
7. Final internal response within 7 days of escalation

Complaints Log:

- Date and nature of complaint
- Investigation findings
- Actions taken
- Resolution outcome
- Complainant satisfaction

15.2 Information Commissioner's Office (ICO)

Right to Complain:

Parents/guardians have the right to lodge a complaint with the ICO if:

- Dissatisfied with DLC's handling of data
- Believe DLC is not complying with UK GDPR
- Breach has occurred and response is inadequate

ICO Contact Information:

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

Cheshire SK9 5AF

Helpline: 0303 123 1113

Website: www.ico.org.uk

DLC Cooperation:

- Full cooperation with any ICO investigations
- Provision of all requested information
- Implementation of ICO recommendations
- Reporting of actions taken

16. POLICY REVIEW AND UPDATES

16.1 Regular Review Schedule

Annual Review:

- Conducted every 12 months from effective date
- Assessment of:
- Effectiveness of procedures
- Changes in legislation or guidance
- Technological developments
- Feedback from community members and parents
- Incidents or breaches

16.2 Trigger Events for Immediate Review

Unscheduled Review Required:

- Significant data breach

- Changes to UK GDPR or Data Protection Act
- ICO guidance updates
- Safeguarding legislation changes
- Technology platform changes
- Significant increase in volume of processing

16.3 Update Communication

Process:

1. Draft updates prepared
2. Community member consultation and feedback
3. Governance approval (if applicable)
4. Parents informed of significant changes
5. Updated policy published on DLC website
6. Community member retraining on changes
7. Implementation date confirmed

16.4 Version Control

Documentation:

- Version number and date
- Summary of changes from previous version
- Approval signatures
- Distribution list

Historical Versions:

- Previous versions archived
- Retained for 7 years
- Available for audit purposes

17. CONTACT INFORMATION

17.1 Data Protection Queries

Data Controller:

Claudia Celi, Founder

Divergent Learning Community CIC

Address: 71-75 Shelton Street, Covent Garden, London, WC2H 9JQ

Email: DivergentLearningCommunity@outlook.com

Phone: 07757749097

17.2 Subject Access Requests

Submit to:

Data Protection Lead (Claudia Celi, Founder)

Email: DivergentLearningCommunity@outlook.com

Post: 71-75 Shelton Street, Covent Garden, London, WC2H 9JQ

17.3 Data Breach Reporting

Internal Reporting:

Immediate notification to: Claudia Celi

Email: DivergentLearningCommunity@outlook.com

Phone: 07757749097 (24/7)

External Reporting (ICO):

Report via: https://ico.org.uk/make-a-complaint/

Or call: 0303 123 1113

18. APPENDICES

Appendix A: Parent/Guardian Consent Form

Appendix B: Privacy Notice for Parents

Appendix C: Privacy Notice for Children (Age-Appropriate)

Appendix D: Document Receipt Log Template

Appendix E: Redaction Quality Checklist

Appendix F: Subject Access Request Form

Appendix G: Data Breach Reporting Form

Appendix H: Community Member Training Record Template

Appendix I: Destruction Certificate Template

Appendix J: Cognitive Profile Template

DOCUMENT APPROVAL

Prepared by:

Name: Claudia Celi

Position: Founder

Date: 25 February 2026

Reviewed by:

Name: Claudia Celi

Position: Founder

Date: 25 February 2026

Approved by:

Name: Claudia Celi

Position: Founder

Date: 25 February 2026

This is a living document and will be updated as procedures are refined and regulatory requirements evolve. All community members are responsible for familiarising themselves with the current version.

Contact & Legal Information

DIVERGENT LEARNING COMMUNITY CIC

Registered in England and Wales | Company Number: 16765759

71-75 Shelton Street, Covent Garden, London, WC2H 9JQ

Email: DivergentLearningCommunity@outlook.com

Tel: 07757749097