DATA PROTECTION , GDPR & INFORMATION SHARING

2026-2027

Group Policy Document

Document Control				
Version	Author	Summary of Changes Approved	Date	Date of Review
V1	DS	New Policy Document	Jun 2026	Jul 2027

CONTENTS

1.0 INTRODUCTION AND SCOPE

1.1 ARK Inclusive Education LTD ("the Company") is committed to protecting the privacy and security of the personal data it processes. This policy sets out our approach to ensuring compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018) .

1.2 This policy also recognises that information sharing is essential for effective safeguarding and promoting the welfare of children and young people . Data protection law is not a barrier to justified information sharing, but provides a framework to ensure that personal information is shared appropriately .

1.3 This policy applies to all employees, contractors, volunteers, and partners who process personal data on behalf of the Company. It covers both routine (systematic) and one-off (exceptional) information sharing .

2.0 DATA PROTECTION PRINCIPLES

2.1 The Company adheres to the seven key principles of the UK GDPR:

- Lawfulness, Fairness, and Transparency: We process personal data lawfully, fairly, and in a transparent manner .
- Purpose Limitation: We collect data for specified, explicit, and legitimate purposes and do not process it in a way incompatible with those purposes .
- Data Minimisation: We ensure personal data is adequate, relevant, and limited to what is necessary .

- Accuracy: We take reasonable steps to ensure personal data is accurate and kept up to date .
- Storage Limitation: We do not keep personal data for longer than is necessary .
- Integrity and Confidentiality: We ensure appropriate security of personal data, protecting it against unauthorised or unlawful processing, accidental loss, destruction, or damage .
- Accountability: We take responsibility for complying with these principles and can demonstrate our compliance .

3.0 LAWFUL BASIS FOR PROCESSING

3.1 The Company will only process personal data where we have a valid lawful basis, including consent, contract, legal obligation, vital interests, public task, or legitimate interests . The lawful bases relied upon include:

- Article 6 (1) (c) – processing is necessary for compliance with a legal obligation to which the controller is subject .
- Article 6 (1) (d) – processing is necessary to protect the vital interests of the data subject or of another natural person .
- Article 6 (1) (e) – processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller .

3.2 Special Category Data (Sensitive Data): The Company will only process special categories of data (e.g., health, ethnicity, religion) where we are legally obliged to do so or are authorised to do so in law . Additional safeguards will be in place to protect this information .

4.0 INFORMATION SHARING: PRINCIPLES AND PRACTICE

4.1 Overarching Principle: Information sharing is vital in identifying and tackling all forms of abuse, neglect, and exploitation, and in promoting children's welfare, including their educational outcomes . Data protection law supports sharing information to safeguard children and young people .

4.2 The Seven Golden Rules for Information Sharing :

- Rule 1: Remember that the UK GDPR and DPA 2018 are not barriers to justified information sharing, but provide a framework to ensure it is done appropriately .

- Rule 2: Be open and honest with the individual (and/or their family where appropriate) from the outset about why, what, how, and with whom information will be shared, and seek their agreement unless it is unsafe or inappropriate to do so .
- Rule 3: Seek advice from other practitioners or your information governance lead if you are in any doubt about sharing the information concerned .
- Rule 4: Where possible, share information with consent. You may share without consent if, in your judgment, there is a lawful basis to do so, such as where safety may be at risk .
- Rule 5: Consider safety and well-being and base your information sharing decisions on considerations of the safety and well-being of the individual and others .
- Rule 6: Ensure the information you share is Necessary, Proportionate, Relevant, Accurate, Timely, and Secure .
- Rule 7: Keep a record of your decision and the reasons for it—whether to share or not. If you share, record what you shared, with whom, and for what purpose .

4.3 Sharing Decisions:

- Necessity and Proportionality: Information should only be shared if it is necessary for the purpose for which it is being shared, and only with those individuals who need to have it .
- Capacity: When considering a child's capacity to exercise their own rights (e.g., consent to share), we will use our discretion and professional judgement. In England, capacity is assessed based on the child's understanding following the Gillick competence test . Safety and wellbeing are paramount, and the duties to report child protection concerns must not be disregarded where the child disagrees .
- Safeguarding Override: The duty to protect a child from serious harm, such as abuse or neglect, is a priority over consent in such situations . Where seeking consent would increase the risk of harm, information may be shared without consent .
- Formal Agreements: Where sharing occurs on a regular basis, a formal Data Sharing Agreement should be in place .

4.4 Sharing with Partner Organisations:

- The Company shares information with a range of partners to fulfil its statutory duties, including:
    - Referring Schools and Local Authorities: To facilitate reintegration and ensure continuity of support.
    - Children's Social Care: To safeguard children and young people.
    - SEND Services: To support children with Education, Health and Care Plans (EHCPs).
    - Health Services (e.g., School Nursing, CAMHS): To ensure essential health services are received .

4.5 Privacy Notices (Fair Processing Notices): We will ensure that up-to-date Privacy Notices are made available to every parent/guardian/carer, or the child/young person if appropriate, to inform them of how their data will be used and shared . These notices will state:

- What data is collected
- How it is used
- How long it is kept for
- With whom it is shared .

5.0 DATA SUBJECT RIGHTS

5.1 The Company will uphold the rights of data subjects :

- Right to be Informed: We provide clear and accessible privacy notices .
- Right of Access: We will respond to Subject Access Requests (SARs) within one month . There is no automatic right for a parent to have access to data held on their child; the presumption is that, by age 12, a child may have sufficient maturity to exercise their own rights . Each request will be considered on its own merits.
- Right to Rectification: We will correct inaccurate or incomplete data .
- Right to Erasure: We will delete personal data where there is no compelling reason for its continued processing .
- Right to Restrict Processing: We will limit the processing of personal data in certain circumstances .

- Right to Data Portability: We will provide data in a structured, commonly used, and machine-readable format .
- Right to Object: We will respect an individual's right to object to processing, including for direct marketing .
- Rights in relation to automated decision-making and profiling .

6.0 DATA SECURITY

6.1 The Company will implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk , including:

- Access Control: Use of strong authentication and principle of least privilege. Access should be limited to those authorised with a need to know .
- Encryption: Encryption of personal data at rest and in transit .
- System Security: Use of firewalls, malware protection, and regular patching .
- Storage: Personal data is stored on secure, password-protected systems, in locked locations if hardcopy .
- Staff Training: All staff will receive mandatory data protection training . This includes understanding the principles in this policy and how to share information securely .
- Caldicott Guardian: An identified senior individual (the Director) will be responsible for ensuring the Company continues to meet its confidentiality and information governance requirements .

7.0 DATA BREACH RESPONSE

7.1 The Company has a data breach response plan to ensure that any personal data breach is detected, investigated, and reported without undue delay. We will notify the ICO within 72 hours where a breach is likely to result in a risk to individuals' rights and freedoms .

7.2 All staff must report any potential data breach, however small, immediately to the Director. Staff must be open and honest and not attempt to cover up what has happened .

RECORD KEEPING AND ACCOUNTABILITY

8.1 The Company will maintain a Record of Processing Activities (ROPA) and conduct Data Protection Impact Assessments (DPIAs) for any high-risk processing .

8.2 We will pay the annual data protection fee to the ICO and will work with the ICO to ensure our compliance is effective .

8.3 All decisions to share (or not share) information will be recorded, including the reasons for the decision, what was shared, with whom, and for what purpose .

8.4 We will retain personal data only for as long as is necessary and in line with our Data Retention Schedule .

9.0 INTERNATIONAL DATA TRANSFERS

9.1 The Company does not currently transfer personal data outside the UK. If such transfers become necessary, we will ensure appropriate safeguards are in place, such as the ICO's International Data Transfer Agreement (IDTA) and a Transfer Risk Assessment (TRA) .

10.0 ROLES AND RESPONSIBILITIES

10.1 The Director (as Data Controller) has overall responsibility for:

- Ensuring compliance with the UK GDPR and DPA 2018.
- The effective operation of this policy.
- Registering with the ICO.
- Responding to Subject Access Requests.
- Managing data breaches and reporting to the ICO.
- Ensuring all staff are trained.

10.2 All Staff are responsible for:

- Understanding and complying with this policy.
- Only collecting and using personal data for legitimate purposes.

- Keeping personal data secure.

- Reporting any data breaches or concerns immediately to the Director.
- Seeking advice if in doubt about sharing information.

10.3 Staff are also expected to:

- Ensure records are accurate and recorded factually, avoiding personal opinions .
- Store data only on official systems and not use personal devices for storage .
- Dispose of data when no longer required, in line with our retention policy .
- Hold confidential conversations in private spaces, not in corridors, cafés, or other public places .

11.0 MONITORING AND REVIEW

11.1 This policy will be reviewed annually by the Director to ensure it remains fit for purpose and compliant with current legislation and best practice guidance, including any updates to the ICO's Data Sharing Code of Practice .

11.2 The effectiveness of this policy will be monitored through:

- Review of any data breaches or near misses.
- Staff training records.
- Regular internal audits of data protection practices.

End of Policy Document